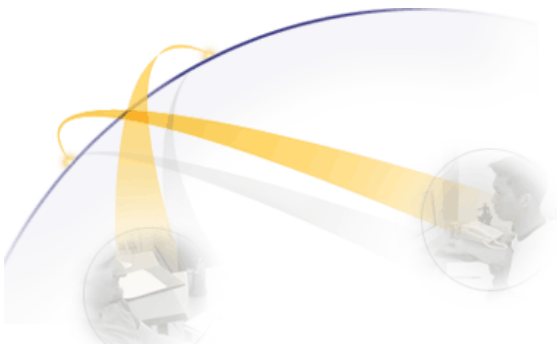
新 E 通产品使用指南

Anywhere,
Anytime,
Anyway,
If you want,
It works.

深大数据通信有限公司
http://www. sddata.com



地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

新E通 系列

产品使用指南

声　明

本公司对本手册的内容保留在不通知用户的情况下更改的权利。其版权归深大数据通信有限公司所有。未经本公司书面许可，本手册的任何部分不得以任何形式手段复制或传播。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

目　录

关于本手册.....5

目的.....5
如何使用.....5
适用对象.....5

第一章　新 E 通系列产品概述.....5

新 E 通产品简介.....6
产品特征.....6
技术要点.....6
硬件接口.....6
物理规范.....6
加密算法.....7
符合标准.....7
新 E 通 VOIP：.....8

第二章　　安装前的准备.....8

环境要求.....8
安全警告.....9
电源.....9
电脑.....9

第三章　硬件安装.....9

新 E 通背板.....9
连接局域网.....10
连接广域网.....10
连接范例.....11

第四章　　配置新 E 通.....11

使用方法和诀窍.....12
基本设置.....13
设置步骤小结.....20
高级设置.....21
安全设置.....26

第五章　工作站配置.....27

网络设置.....28
WINDOWS 工作站设置举例.....28

第六章　防火墙设置.....31

设置基础.....31

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　　传真：86-755-83268498
网址：www.sddata.com　　邮编：518029

设置概述.....31
对局域网用户的管理.....33
对新 E 通用户的管理.....34
定义组策略.....35
定义外网访问许可.....37
NAT 设置.....38
恢复缺省设置.....39
日志.....39

第七章 路由设置.....40

查看当前路由表.....40
配置概述.....41
手工设置路由.....42

第八章 管理新 E 通.....42

查看所有连接.....42
查看当前网络配置.....43
检测广域网连接.....44
检测局域网连接.....44
PING 命令详解.....45
账号管理.....45
口令.....46
忘记口令.....46

安全性详述.....47

系统的安全性概述.....47
新 E 通架构.....48
隧道技术.....48
加解密技术.....48
使用者与设备身份认证技术：.....48
新 E 通的 IPSEC 架构.....49
加密机制.....50
硬件加密过程.....51
新 E 通 FIREWALL 2.0 基于 IPTABLES 的防火墙：.....51
防火墙的分组管理功能：.....52
新 E 通防火墙的特点：.....52
对外的安全防范.....53

常见问题解答.....54

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

关于本手册

目的

本手册提供了新 E 通系列产品的安装使用说明（包括硬件安装和软件安装），随新 E 通产品一起交付给用户。

如何使用

本手册分为硬件安装、软件安装两大部分。使用者可按照本手册所描述，自己完成所有的设置。如没有特别说明，本手册中采用的一些标志含义为：

加粗	**root**	表示用户输入命令
注意	**NOTE**	表示重点提示
加粗斜体	***Your Name***	表示需要您的输入，其输入内容需要替换成符合您自己系统的具体内容
特别提示		本提示在于对某些用户容易误解的内容作出加重的提示信息
	警告	表示需要特别注意，许多会跟设备和数据的功能和可靠有关，务必仔细注意
	诀窍	按照该提示可能会使您节约一点时间
	总结	表示对上述内容的一个小结，常常可以使您及时明白上一段所描述内容及其目的

本手册共计八章。

如果您只是普通用户，只需阅读一到五章即可。

如果您需要更高级的功能，例如更改出厂设置，手动配置根据您自己实际网络结构而决定的某些参数，或更深入更灵活的使用新 E 通产品的强大功能，请阅读第六章以后的内容，您将能设置防火墙，路由信息等功能。

适用对象

本手册适用于购买我公司新 E 通产品的用户。同时要求使用者需要具有 TCP/IP 的基础知识和一定的网络知识，熟悉电子设备的保护和使用。

第一章　新 E 通系列产品概述

本章主要描述了新 E 通产品的功能和物理规范。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

新 E 通是集成有多种广域连接、局域网连接、透明代理上网(作为共享上网用)、动态企业虚拟专网的高技术网络互联产品。它实现了企业所有上网节点都为动态 IP 上网并组成网状拓朴结构的功能。

新 E 通产品简介

为了实现现在线路的连接，我们提出一种全新的解决方案，就是利用我们的新 E 通系列产品。它最大的特点就是费用低，稳定可靠，无需专线，无需固定 IP 地址，可以支持多种上网方式，如拨号、ISDN、ADSL。

产品特征

新 E 通是解决网络安全传输的最高效，最节省的组网技术。

- 新 E 通能使用动态 IP 接入 Internet 的 LAN 之间进行互联。
- 新 E 通能形成网状的网络连接，通讯无中心瓶颈，构建高效的即时通讯平台；
- 以最低成本接入，最低通讯成本提供高性能、高可靠性的企业专网的计算机网络技术。
- 新 E 通支持 ADSL、 ISDN、 DDN 、Dial-up 方式以及静态/动态 IP 接入。在相同的通讯带宽下，节省 80%通讯费用。
- 新 E 通能使普通企事业单位也能通过 Internet 组建自己的企业专网。使企业所有在局域网上的网络应用以最低的成本应用至 Internet 所及的范围。

技术要点

- 协议：TCP/IP
- 基于 IPSec 国际标准
- 完善的路由功能
- 完善的宽带代理服务器。NAT/PAT 地址转换技术保护内部网络。
- DHCP 服务器
- DNS 服务器
- 设备是一个高性能的防火墙
- 内置 PPPoE
- Telnet or VT100 终端控制端口命令行

硬件接口

- Console 接口：系统配置及系统监测，通过 RS-232 (9600, 8N1)进行通讯
- 局域网接口：Ethernet Interface, 10/100BASE-T
- 广域网接口： Ethernet Interface 10/100BASE-T) / PPPoE 通讯口接口 (用于接 ADSL Cable Modem)
- 广域网接口： RS-232, 外置 Dial-up Modem / ISDN TA
- DMZ 区：部分型号支持。

物理规范

- 输入电压： 110V~230V
- 功率：最大约 40W

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

- 使用环境温度：0~45 ℃
- 使用环境湿度：5~95%

加密算法

数据传输可自由选择

- AES/128 位加密算法
- 3DES/168 位加密算法
- SERPENT/128 位加密算法
- BLOWFISH/128 位加密算法
- TWOFISH/128 位加密算法
- 国家密码委员会指定的硬件加密卡或第三方算法

保证数据完整可自由选择

- MD5-96
- SHA1-96
- SHA2-256
- SHA2-512

身份认证支持

- RSA 2048
- Pre-share Key

符合标准

- RFC2401 Security Architecture for the Internet Protocol
- RFC2411 IP Security Document Roadmap
- RFC2402 IP Authentication Header
- RFC2406 IP Encapsulating Security Payload (ESP)
- RFC2367 PF_KEY Key Management API, Version 2
- RFC2407 The Internet IP Security Domain of Interpretation for ISAKMP
- RFC2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC2409 The Internet Key Exchange (IKE)
- RFC2412 The OAKLEY Key Determination Protocol
- RFC2528 Internet X.509 Public Key Infrastructure
- RFC2085 HMAC-MD5 IP Authentication with Replay Prevention
- RFC2104 HMAC: Keyed-Hashing for Message Authentication
- RFC2202 Test Cases for HMAC-MD5 and HMAC-SHA-1
- RFC2207 RSVP Extensions for IPSEC Data Flows
- RFC2403 The Use of HMAC-MD5-96 within ESP and AH
- RFC2404 The Use of HMAC-SHA-1-96 within ESP and AH
- RFC2405 The ESP DES-CBC Cipher Algorithm With Explicit IV
- RFC2410 The NULL Encryption Algorithm and Its Use With IPsec
- RFC2451 The ESP CBC-Mode Cipher Algorithms

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

I RFC2521 ICMP Security Failures Messages

新 E 通 VOIP：

- 符合中国 IP 标准；
- 符合最新国际标准及相关建议；
- 符合 H.323/v2,MGCP 等全套 IP 语音网关标准；
- 支持 G723.1(5.3kb/s,6.3kb/s),G729(8kb/s),g.711 等压缩算法；
- 可与 CISCO5300,26/36 系列 、NetMeeting 等主流厂商的 VOIP 网关、GateKeeper 设备互联互通，被主流 GateKeeper 管理。

第二章　　安装前的准备

本章介绍了安装之前的准备工作以及一些注意事项。

环境要求

系统可在如下的环境下使用。

输入电压： 210V~230V

功率：　　最大约 40W

使用环境温度： 0 ~35 ℃

使用环境湿度：5~95%

为保证系统能长期稳定的运行，应保证电源有良好的接地措施，防尘措施，及在如下环境条件下使用：

输入电压： 210V~230V

使用环境温度：15 ~ 25 ℃

使用环境湿度：5 ~ 85%

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

安全警告

本系统不能在有酸性，碱性环境，强磁场等恶劣环境下使用。在这类环境下使用本系统不保证能正常使用。导致的系统物理损坏亦不在本产品的品质保证之中。

这是甲类的资讯产品，在居住的环境中使用时，可能会造成无线电干扰，在这种情况下，使用者会被要求采取某些适当的措施。.

电源

本产品采用国际化设计，使用交流 100V 到 240V 电源。在您接通电源之前，请保证您的电源有良好的接地。

电脑

在配置本产品之前，您需要配备一个装有超级终端软件的电脑，同时需要该电脑具有至少一个 9 针的 com 接口。这样配置的电脑现在很容易找到。如果您运行的是 Microsoft 公司的 Windows95，Windows98 或 Windows 2000 操作系统，您还需要检查是否安装了“超级终端”这个程序。此外，您还可以用一些标准的终端程序，例如 neterm 来进行设置新 E 通。我们推荐您使用该软件。

第三章　硬件安装

本章介绍了新 E 通的硬件安装。包括：

- 连接配置线
- 连接局域网
- 连接广域网

新 E 通背板

新 E 通的背板如下图所示。将 Console 口和一台 PC 机的串口用随机电缆连接起来。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

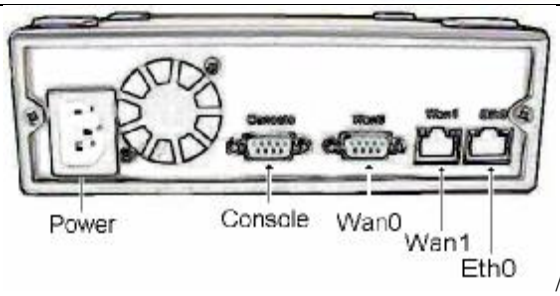


图 3－1 新 E 通 GW2000 背板图

连接 Console 线

通过新 E 通随机带的 RS-232 通讯电缆，把新 E 通的系统配置/监控接与控制终端进行互联，并设定控制终端的通讯参数如下：

通讯串口：(跟据终端实践所接通讯串口而定，可能是串口 COM1，也可能是串口 COM2。)

波特率：9600

数据位：8

停止位：1

奇偶校验：N

一般用普通电脑作为控制终端。把 Console 电缆一端直接接在新 E 通 GW 2000 背面的 Console 接口上，另外一端连接到电脑的 COM 口上。

系统配置完成后，启动新 E 通，终端会看到有关新 E 通的启动信息和系统提示。

连接局域网

使用标准 RJ-45 插口的以太网接口。

将新 E 通 的 Eth0 端口用 RJ45 网线连接到本地局域网中。

连接广域网

对于用 Modem 或是 ISDN (只支持外置的 TA 设备)的接口，是一个标准的 RS-232 接口，通过与 Modem 或 ISDN TA 的串口通讯接口与新 E 通中标注 Wan0 的接口相联。

如使用 ADSL 上网，用双绞线与 ADSL CABLE MODEM 上的 LAN 接口连接到新 E 通产品上标注 Wan1 的接口进行互联。

如使用 DDN、Cable Modem、宽带上网的，用双绞线与新 E 通 WAN1 端口相连。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

连接范例

用 ADSL 连接上网。

第一步 打开新 E 通包装，取出新 E 通设备，电源线，console 线；

第二步 把 Console 线一端连接到新 E 通的 Console 上，另外一端接在电脑的 Com 口上。在此过程中，新 E 通和电脑都要求不接电源。

第三步 把 ADSL 网线连接到新 E 通的 WAN1 上。

第四步 把从局域网的 HUB 或交换机上引出的网线连接到新 E 通的 Eth0 上。

以上连接完成。先启动电脑，启动超级终端应用程序。硬件安装完成。打开新 E 通电源，可以看到电源指示灯和系统自检指示灯亮。

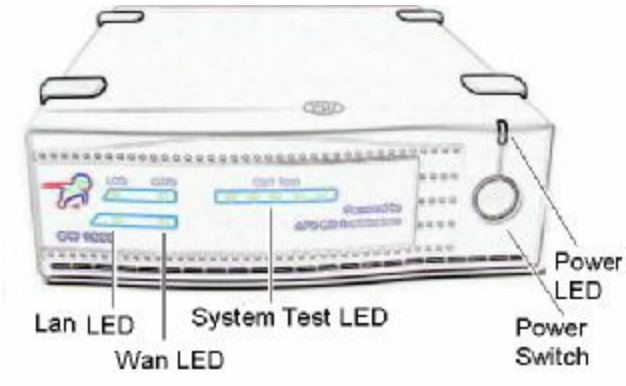


图 3－2 新 E 通面板图

第四章 配置新 E 通

本章主要介绍如何配置新 E 通。通过本章，您可以学会如何让新 E 通开始工作。本章讲述的是新 E 通的基本配置。其他关于防火墙或路由的配置，您需要阅读以后的章节。

本章主要有三大部分：

- 基本设置
- 高级设置
- 安全设置

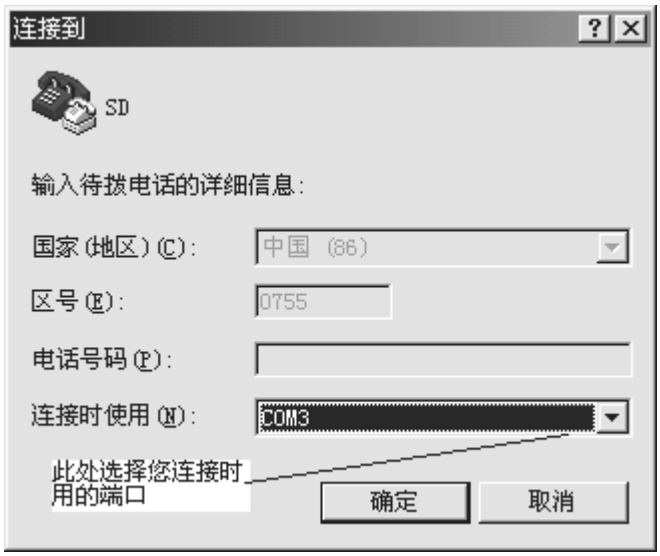
如果您是一般用户，您可以只读基本配置部分。完成此部分工作，新 E 通就可以正常工作了。系统缺省设置中预设了加密算法和验证算法。如果您需要更详细的了解新 E 通的其他设置，您可以继续阅读高级设置部分和安全设置部分。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

使用方法和诀窍

超级终端

我们以 Windows 98 为例。在开始——程序——附件——中，有一个超级终端的软件。您需要启动它。如上一章所示，在新 E 通和电脑之间，您需要用 console 线连接起来。如果您的 console 线连在电脑的 com1 口上，在超级终端中就需要选择 com1 口。

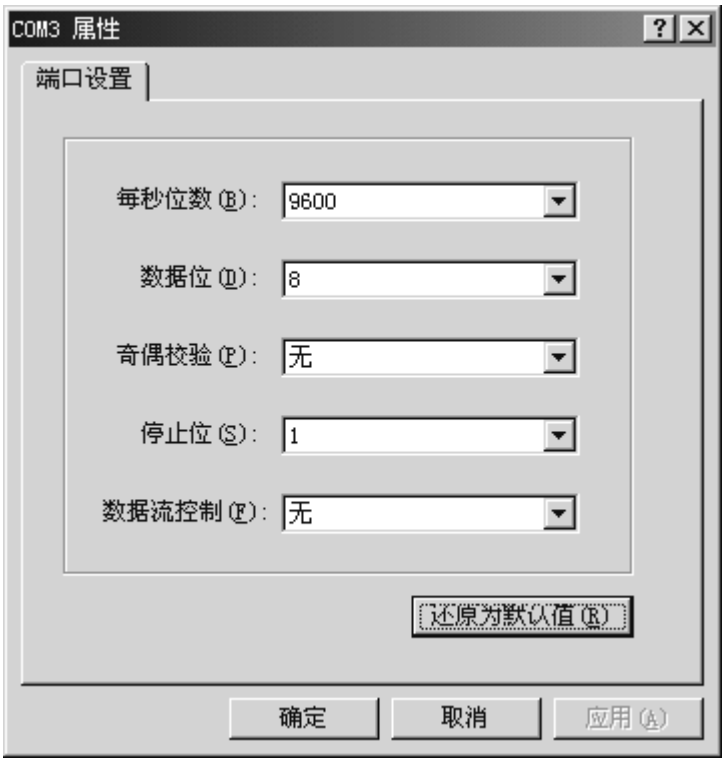


选择端口后，选择确定，您需要设置通讯的

波特率为 9600
数据位 8
奇偶校验 无
停止位 1
数据流控制 无

注意：在不同的系统中，上述名词可能会不一样。
例如在繁体中文 windwos 中，超级终端叫超级终端机。附件叫附属工具。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029



Tab 键自动完成

您在设置新 E 通的时候，您可以使用 tab 键来完成命令的输入。例如，您需要输入 setup 时，只需要输入 set，然后按 tab 键，系统会自动完成 setup 整个字串的键入。这有助于您忘记某些命令时系统自动帮您完成输入。

注意： 新 E 通系统只能完成当前支持的唯一的命令。如果您键入的未完成字母有多种可能，系统将无法确定您需要的哪一个，而列出所有可能的命令。

Ctrl＋P 重复上一条命令

您在设置新 E 通的时候，您可以使用 ctrl 键加 P 键重复上次输入的命令。

NetTerm

注意：如果您需要手动配置一些参数，例如手动配置路由和手动配置防火墙，您可能会使用新 E 通自带的编辑器。由于超级终端设计上的原因，我们强烈建议，使用随机光碟上的 NetTerm 软件来替代超级终端。

使用超级终端时，可能在编辑路由表或防火墙规则时，上下左右的方向键会失效。这种情况下建议使用 NetTerm。它是一个很著名的远程登录和终端工具，支持 VT-52, VT-100, VT-220, VT-320, QNX 2, TVI-925, WYSE-50, IBM-3101, IBM-3151, IBM-3161, IBM-3163, XTERM, SCO ANSI, ANSI, Nixdolf BA-80, and FTTERM。

基本设置

注意： 以下所列系统显示信息可能会因为新 E 通版本的不同而略微有些差异。但以下所列操作适用于所

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

有的版本。

系统正常引导启动(接电源开关并等待约 40 秒左右时间)后。输入配置系统帐号：

Login：***root***

Password：***gw1admin***

系统提示符为 APNGW＃。

此时输入 help 可以看到：

```
AUTHCYBER.COM APN GW    HELP
    Copyright (C) 2001-2016, All right reserved

setup:      To config basic configuration of apngw, you should do this
             first if you have not do this yet.

advconf: Advantage config, to config APN GW Manual, or restart it.
             config DNS, DHCP, turn switch TELNET, FIREWALL and so on.
             You should do this after you finished config basic config.

fwconf:    APN Firewall configuration and management. Include filter,
             Port forward, NAT, LOG function.

Local time (GMT): Tue May 21 09:31:30 UTC 2002

Adjust Date if you need.
  Usage:
        # date -s <new_datetime>)     ## date eg: "Apr 28 4:50:23 2002"
        # hwclock --systohc              ## So that write to CMOS
*****************************************************************

[APNGW /]#
```

输入：

setup

此时会启动设置菜单，如下所示：

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

```
                    APN GW CONFIG

AUTHCYBER.COM APN GW1 CONFIG
    Copyright (C) 2001-2016, All right reserved

You should read the INSTALL MANUAL first,   Enter: setup for this
If you are first time to config it on the step 1,2,3,4

The APN GW configuration choices are:

1 - APN GW LICENSE   (VDOMAIN/VHOST/LICENCE/VPUBKEY)

2 - APN LAN NETWORK (LAN IP/MASK)

3 - WAN LINK            (ADSL/DDN/ISDN/Dial-up)

4 - SAVE RUN_CONFIG TO START_UP_CONFIG

0 - EXIT CONFIGURATION:   Exit to system prompt.

Your choice?
```

对于新机，应按照 1，2，3，4 的次序来进行系统配置。其中各项的作用：

1. 新 E 通 Licenses：有 VDOMAIN, VHOST 及 VDOMAIN 及 VHOST 对应用的 Licenses 项组成。要互相通讯的结点之间用共同的 VDOMAIN 项，相同的 VDOMAIN 结点之间的 VHOST 不能重用，即同 VDOMAIN 之中，每个结点都要有不同的 VHOST，Licenses 是一个 16 位的 ASCII 字符，其包装中会有提供。每台新 E 通机都要其唯一的 License。由新 E 通提供商提供。

   配置内容：

   Every APN GW have a unique VDOMAIN/VHOST License
   APN GW at the same VDOMAIN and Authenticate PSK
   can communication to each other.

   APN GW VDOMAIN(Default:unkonw): ***your domain***
   APN GW VHOST(Default: unknow): ***your host***
   APN GW LICENCE (Default: APNLICECESNUST24BYTES):***your license***
   Authenticate PSK(Default: public):***pre-share Key***

   ** Summary of what you entered **
   AUTHBY   = Pre-share-key

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

APN GW VDOMAIN : demo
APN GW VHOST : demohost
LICENCES : WrWtg4gk6O8rPowd7qqn4j
Authenticate PSK : public

Accept these settings and adjust configuration files (y/n)? ***y***

新 E 通要能够通过 IKE 方式协商密钥，必须具有以下两个条件：两端配置有匹配的 POLICY；两端配有匹配的安全策略（此安全策略当然不用配置验证与加密密钥）。在 POLICY 中用户事先定义了一些 IKE 协商的自保护措施，他们包括：协商报文的加密算法，验证方法，散列算法，使用的 DH 组标识，安全连接的生存时间等等。验证方法的定义非常重要，我们以 pre-share 这种验证方法为例，这是一种秘密密钥验证方法。

2. 新 E 通 Network：局域网设置，用于设定新 E 通的局域网口参数，现在的新 E 通提供的是 100Base-T Ethernet 接口。配置新 E 通的 IP 地址及其子网掩码。局域 IP 地址可为任何有效的 IP 地址，但建议使用保留的 IP 地址段：

A 类地址：10.0.0.0 ~ 10.255.255.255.0

B 类地址：172.16.0.0~172.31.0.0

C 类地址：192.168.0.0 ~ 192.168.255.255

注：因为 172.31.250.0 ~ 172.31.250.255 作为 APN GW 保留的初始地址，故这个网络的地址也不要使用。

同 VDOMAN 的每个结点的网络地址不能重复，否则会导致相同网络地址的结点不能与其它任何结点进行通讯，也不能上 Internet 网络。

举例如同：如同 VDOMAIN=Olym VHOST=shenzhen 的结点机 IP 地址为：192.168.0.10/255.255.255.0, 那么其它结点比如: VDOMAIN=Olym VHOST= guanzhou 的 IP 地址否则不能为：192.168.0.xxx/255.255.255.0。

配置内容：

APN GW IP Address
Enter the IP address of the Internal network
(default 192.168.0.63): **192.168.250.10**

APN GW IP Address Netmask
Enter the IP Netmask of connected to the internal network
(default 255.255.255.0): **255.255.255.0**

** Summary of what you entered **
APN GW IP Address: 192.168.250.10
Netmask: 255.255.255.0

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

Accept these settings and adjust configuration files (y/n)? ***y***

注：上面文件中如下的内容是用户输入内容。是接用户实践要求输入的。子网掩码请设为：255.255.255.0。

192.168.250.10

255.255.255.0

注意： 我们强烈建议使用者不要使用诸如 202.96.10.10 这样一类的公网的 IP 地址作为自己内部局域网的 IP 地址。

3. WAN LINK：是配置广域联接的选项。支持的广域联接接口有：外置 56K Modem 拨号，ISDN TA 拨号，ADSL 的 PPPoE 接口，及 DDN, Ethernet 接口。进入本项后。会要求输入广域联接方式，四个接网方式在任一时刻只能用其中的一种方法上网，当配好一种方式上网后别的方式自动失效。

```
APN WAN: Select the way to link to Internet

1 - Dialup        : Use Extend Modem Link to Internet
2 - ISDN          : Use ISDN TA Link to Internet Must a extend device
3 - ADSL          : ADSL Link to Internet
4 - DDN/FIX IP    : DDN or other lease line link to Internet have fix ip
0 - EXIT TO Main: Return to main menu

Your choice?
```

选取 ***1*** —Dialup， 进行拨号上网方式的有关配置。

系统接线为：Modem 的 RS-232 电缆与新 E 通中标有 *MODEM* 字样的接口，另一头与 MODEM 进行互联。

配置内容：

Enter the phone number of your ISP

Phone Number: **163**

Enter your dial-up username

Username: ***163uid***

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

Enter your dial-up Password
Password : ***163passwd***

** Summary of what you entered **
Dial Up Number : 163
Dial Username : 163uid
Dial Password : 163passwd

Accept these settings and adjust configuration files (y/n)? ***y***

注意：上面文件中如下的内容是用户输入内容。是拨号的对端电话号码及分配的帐号。对于是通过分机上网的，要在被拨的电话号码前加，拨外线的号码及一个“，”号。如拨外线的号为“9”，拨 163 的电话可以拨：“9,163”。

选取 ***2*** —ISDN ，与 ISDN TA 进行互联的方式。

系统接线为：Modem 的 RS-232 电缆与 APN GW 中标有 *MODEM* 字样的接口，另一头与 MODEM 进行互联。此接口与 MODEM 拨号上网是用同一个接口，故任一时刻只能用其中的一个上网。

配置内容：

Enter the phone number of your ISP
Phone Number: **96169**

Enter your dial-up username
Username: ***96169dialupuid***

Enter your dial-up Password
Password : ***96169dialuppwd***

** Summary of what you entered **
Dial Up Number : 96169
Dial Username : 96169dialupuid
Dial Password : 96169dialuppwd

Accept these settings and adjust configuration files (y/n)? ***y***

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

注意：上面文件中如下的内容是用户输入内容。是拨号的对端电话号码及分配的帐号。对于是通过分机上网的，要在被拨的电话号码前加，拨外线的号码及一个“，”号。如拨外线的号为“9”，拨 96169 的电话可以拨：“9,96169”。

选取 ***3*** —ADSL，与 ADSL Cable Modem 进行联接的方式。

系统接线为：新 E 通的标有 ADSL/DDN 字样的接口通过标准交叉双绞线与 CABLE MODEM 进行联接。

配置内容：

Enter your PPPoE user name
Username: (default uid@163.gd): ***your_username@163.gd***

Enter your ADSL Password
Password : ***password***

** Summary of what you entered **

PPPoE User name : your_username@163.gd
Password : passwdhere

Accept these settings and adjust configuration files (y/n)?***y***

注意：上面文件中如下的内容是用户输入内容，这部分申请 ADSL 时由电信提供的用户名与密码。

your_username@163.gd
password

特别提示：本项设置主要是针对虚拟拨号的用户。对于部分专线的 ADSL 用户，由于您的 IP 是固定的，所以您设置广域网连接的时候，一定要选择用 DDN 连接这一项。

选取 ***4*** —DDN， 通过 Ethernet 的联接方式。

系统接线为：新 E 通的标有 ADSL/DDN 字样的接口通过标准交叉双绞线 Route 的局域网联接，或是通过以太网接入可上互联网的 HUB。此接口与 ADSL 接口共用一个物理 RJ45 接口。

配置内容：

DDN IP Address
Enter the IP address of the Internal network
(default 172.168.250.250): **202.104.177.177**

APN GW IP Address Netmask

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

Enter the IP Netmask of connected to the internal network
(default 255.255.255.0): **255.255.255.240**

** Summary of what you entered **
DDN IP Address: **202.104.177.177**
Netmask: **255.255.255.240**

Accept these settings and adjust configuration files (y/n)? ***y***

注意：上面文件中如下的内容是用户输入内容，这部分是分配给新 E 通广域 IP 地址。实践使用中按由网管分配的 IP 进行分配。

特别提示：对于某些 ISP（例如长城宽带），提供给用户的地址可能需要绑定网卡的 MAC 地址。对于这种情况，请一定注意查看新 E 通的 MAC 地址后告诉提供商重新绑定。可以用 ifconfig 命令查看。

4. Save Run_Config to Start_up_Config

您做了设置之后，运行无误后，别忘了选择此项存入新 E 通。如果您没有选择此项功能，那末您的本次的设置在启动时将丢失。

注意： 新 E 通系统运行时，所有的程序运行于随机存储器之中。您做的设置只是对当前的操作有效。如果您需要把当前正确的设置保存下来，您一定不要忘记选择此项存于新 E 通系统中。否则系统启动后会自动恢复到上一次存取的状态。

设置步骤小结

如果您是首次使用新 E 通，下面的小结可能让您在 5 分钟内学会使用。我们以设置 ADSL 虚拟拨号上网为例。

第一步 用 root 作为用户名，gw1admin 作为初始密码进入系统，键入 setup；
第二步 选择 1，按《最终用户许可协议》上所示内容输入 vdomain，vhost 和 licenses；
第三步 选择 2，设置连接内部网络的 eth0 接口卡的 IP 地址和子网掩码；
第四步 选择 3，再选择 ADSL，输入用户名和密码；
第五步 选择 4，保存以上设置；
第六步 重新启动新 E 通（直接按下电源按钮，然后过两秒后再开）。设置完毕。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

高级设置

新 E 通的配置模式

新 E 通有三种配置模式。在每个模式里都有相应的命令。下表所列的命令说明了新 E 通的所有模式。

命令模式	功能	系统提示	退出
Setup	普通设置模式。登录后能即进入此模式，能执行 setup 设置新 E 通的基本参数。	APNGW#	exit
Advconf	高级设置模式。在设置模式下输入命令进入此模式。可以设置新 E 通的高级参数。	CONF>	exit

高级设置支持以下几种配置命令：

APNGW#**help**

APNGW : Advantage APN GW Setting and Management
DHCP : Dynamic Host Configuration Protocol Server Configuration and Management
TELNET : Telnet turn on/off
DNS : Domain Name Service Configuration and Management
USER : User Management
FIREWALL: Firewall Configuration, Must set APN GW as manual way to use this function.
PORTFWD: Port Forward Configuration
ROUTE : Additional route setting

CONF>

此时的提示为 CONF>。在此状态下能支持以上命令。其中：

APNGW： 用于设置新 E 通进程的配置和管理。
DHCP： 打开或关闭 DHCP 服务。
TELNET： 用于打开和关闭 Telnet。
USER： 用户管理，可以更改用户名、密码、增加用户。
FIREWALL： 配置防火墙。定义防火墙策略。
PORTFWD： 配置端口转发。可以把当前 IP 地址的某一个端口转发到内部网络的其中一个机器上。
ROUTE： 配置路由。

通用信息：

每个配置都大致有三个公用命令：

start： 开始此项服务；
stop： 停止此项服务；
save： 保存当前配置。如果不选择 save，那么下次启动，当前的配置将全部丢失。
所以，配置的顺序应该是：

config 或 edit 当前配置……start（stop）开始或停止此项服务……save 保存配置

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

注意： save 存盘时，会把状态一起保存。就是说，如果您配置了某项服务，但是您如果没有启动它的话，那么即使您存盘了下次启动时候还是不会启动。应为它没有把启动或停止的状态保存。

如何使用 DHCP

新 E 通系统支持 DHCP，但该功能在出厂设置时是关闭的。您如果需要使用 DHCP，您需要在进入新 E 通系统设置状态下键入如下命令。

使用 root 登录，在提示符 APNGW#下键入：

APNGW# ***advconf***

系统会提示：

APN GW advantage Network Configuration

Type help to list available command.

Type the command to enter certain function menu.

CONF>

输入 dhcp，可进行 dhcp 的设置。键入 help 可查看所支持的命令。

CONF> ***dhcp***

DHCP config menu, available command is: {start|stop|config|save}

CONF_dhcp>***help***

Your can use: {start|stop|config|save|exit}

CONF dhcp>***config***

DHCP CONFIGURATION

NETWORK: 192.168.1.1

NETMASK:255.255.255.0

Input your DHCP subnet ip range, first ip address:

(default 192.168.1.0): ***192.168.1.10***

Input your DHCP subnet last ip address:

(default 192.168.1.255): ***192.168.1.200***

CONF_dhcp>***start***

Starting dhcpd:

Address range 192.168.1.10 to 192.168.0.100,netmask 255.255.255.0 spans multiple subnets!

OK.

CONF_dhcp>***save***

通过以上命令，成功配置 dhcp，其分配地址 192.168.1.10 到 192.168.1.100。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

说明： DHCP 支持以下几个命令：start, stop, config, save, exit。其含义如下：

start：开始 dhcp，注意此时您应该配置好了 dhcp。

stop：停止 dhcp，注意此时您应该配置好了 dhcp。

config：配置 DHCP。需要设置 DHCP 开始的地址，中止的地址。

save： 把配置文件保存起来。如果您不保存，那么下次启动时会丢失本次配置。

exit：退出配置模式。

如何配置 DNS

新 E 通可以作为 DNS 服务器使用。但是出厂时，该功能是关闭的。这是从安全角度考虑。一般 DNS 也是 Internet 上容易受到攻击的服务之一。一般情况下，如果您知道当地的 ISP 提供的 DNS，建议用户不要打开本选项。

使用 root 登录，在提示符 APNGW#下键入：

APNGW# ***advconf***

CONF>***dns***

DNS(Domain Name Service)setting, available command is :{start|stip|config|save}

CONF_dns>config

You must setting APN License and LAN IP address before build DNS!

(您需要先配置新 E 通的 Licenses 和内部网络接口的 IP 地址)

配置之后，用 start 激活，再用 save 保存，DNS 就配好了。如果您配置了 DNS，在下一章中的客户端设置中，您就不需要知道 ISP 的 DNS 的地址了。只需输入新 E 通的内部接口的 IP 地址即可。

如何使用 Telnet

新 E 通系统支持 telnet，但该功能在出厂设置时是关闭的。您如果需要使用 telnet，您需要在进入新 E 通系统设置状态下键入如下命令。

使用 root 登录，在提示符 APNGW#下键入：

APNGW# ***advconf***

CONF>**telnet**

TELNET config menu, available command is {start|stop|save}

CONF_telnet>***start***

THIS WILL ALLOW ROOT TO LOGIN APN GW VIA PRIVATE NETWORK OR INTERNET.

OPEN THIS SERVICE MAY CAUSE SERIOUS SECURITY PROBLEM. BE SURE CHANGE ROOT PASSWD AND SAVE IT BEFORE YOU USE THIS FUNCTION.

Note:

use: advconf user passwd, advconf user save, to change root password.

Be sure to open telnet service (y/n)? ***y***

Starting inetd: OK

CONF_telnet>***save***

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

说明： telnet 支持以下几个命令：start, stop, save, exit。其含义如下：

start：打开 telnet 功能；

stop：关闭 telnet 功能；

save： 把配置保存起来。如果您不保存，那么下次启动时会丢失本次配置。

exit：退出配置模式。

警告：打开 telnet 可能会存在安全隐患。如果打开，您切记要更改 root 的密码。

在出厂设置中，telnet 是关闭的。如果您一旦打开，就可以通过远程登录到新 E 通对其进行设置。所以，您一旦打开该功能，需要更改 root 及其密码以确保新 E 通系统的安全。关于密码的设定，请参考《管理新 E 通》这一章。

如何用户管理

新 E 通可以配置用户的密码和帐号。您可以在这里增加新的账号或更改删除账号，或更改密码：

[APNGW /]#***advconf***

CONF>***user***

User Mangement,available command is :{add|del|list|passwd|save}

CONF_usr>

改变登录密码

CONF_usr>***passwd***

IF YOU ARE GONIGN TO CHANGE ROOT PASSWD, BE SURE REMEMBER YOUR ROOT PASSWORD.IF YOU LOSS IT AND YOU WILL NEVER LOGIN APN GW AGAIN

Press a key to continue….

User Name: ***root***

Enter the new password(minimum of 5,maximum of 8 characters)

Please use a combination of upper and lower case letter and numbers.

Enter new password:*****

Re-enter new password:*****

Password changed.

增加一个用户

CONF_usr>***add***

New User Name: ***guest***

Change the password for guest

Enter the new password(minimum of 5,maximum of 8 characters)

Please use a combination of upper and lower case letter and numbers.

Enter new password:*****

Re-enter new password:*****

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

Password changed.

配置之后，用用 save 保存。

如何配置端口转发(只是限于基于 APNOS1.0 版本) 其他设置请参考防火墙设置

新 E 通可以把某一个端口转发到内网中其中一台机器。例如可以把 web 服务的 80 端口、或 telnet 服务 23 端口转发到内网的另外一个或多个机器。这样做主要是对于那些需要把 IP 地址充分利用的用户。例如部分地区的 ADSL 用户会得到一个固定的 IP 地址，可以把该地址用于其他服务。

CONF>***portfwd***
To use this function
Manual Firewall Setting, available command is: {config|start|stop|save}

CONF_portfwd>***config***
DNAT: Port forward
==========
No DNAT rules defined

Format: service_name|{tcp|udp}:port_num->dest_ip[:port[-port]]
available: {www|telnet|ftp|pop3|smtp} or
{tcp|udp}:<port_Number>
eg1, telnet->192.168.32.250
eg1, tcp:8080->192.168.32.240:80
##{add|del} for switch input mode, exit to break input
****
ADD >
选择配置后，缺省是 ADD 方式。这里只有两种方式：

ADD> 增加一条转发配置，用 add 可以切换到此方式；

DELETE > 删除一台转发配置，用 del 可以前后到此方式。

在 ADD 方式下，您可以加入您需要转发的目的地址和端口。系统提供了 www/telnet/ftp/pop3/smtp/作为标准的端口。您可以输入名字而无需输入端口号。例如，此时新 E 通的公网地址是 202.96.134.123，我们需要把该地址作为 WEB 服务。但是提供 WEB 服务的服务器在内网里面，其 IP 地址是 192.168.32.250。您需要如下设置：

[APNGW /]***advconf***
CONF>***portfwd***
CONF_portfwd>***config***
….
ADD >***www->192.168.32.250***
DNAT: Port forward
==========
www->192.168.32.250

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

Format: service_name|{tcp|udp}:port_num->dest_ip[:port[-port]]
available: {www|telnet|ftp|pop3|smtp} or
{tcp|udp}:<port_Number>
eg1, telnet->192.168.32.250
eg1, tcp:8080->192.168.32.240:80
##{add|del} for switch input mode, exit to break input
****

ADD >***exit*** #要退出配置模式。
CONF_portfwd>***start*** #服务
CONF_portfwd>***save*** #设置存盘。

如果您需要删除以上配置，您只需要在上面的 ADD 方式下输入 **del** 后转换到 ADD>del 方式后采用同样的配置。

注意：在配置端口转发之后，您需要先 start 此项服务之后，再 save。因为 save 不光是保存了您的配置，还把您是否启动该项服务的状态也保存了下来。

诀窍：

您可以一次键入命令完成最终的具体设置模式的命令。

例如：您需要配置 telnet，您可以使用：

APNGW#***advconf***
CONF>
CONF>***telnet***
CONF_telnet>

这时您可以配置 telnet。但您使用以下的方式更简便：

APNGW#***advconf telnet***
CONF_telnet>

诀窍：

在 CONF>模式下，或在具体应用设置模式下，您可以使用 help 来查看所有支持的命令。例如

CONF_telnet>***help***
You can use:{start|stop|save|exit}

其他两项，如何设置路由和如何设置防火墙，我们将在后面的章节中进行更详细的陈述。

安全设置

新 E 通的安全设置

新 E 通支持多种加密算法。

命令模式	功能	系统提示
ipsec config	设置通讯的加密算法。	APNGW#
ipsec auto status	查看 IPSec 的状态。	APNGW#

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

[APNGW /]#***ipsec config***

Available ESP Encrypt

No.	Name	Speed	Comp.	Full_Name
1	null	89		NULL
2	aes	55		AES/128
3	3des	35		3DES/168
4	serpent	57		SERPENT/128
5	blowfish	63		BLOWFISH/128
6	twofish	62		TWOFISH/128

Available Authentic

No.	Name	Speed	Comp.	Full_Name
1	md5	56		MD5-96
2	sha1	44		SHA1-96
3	sha2_256	42		SHA2-256
4	sha2_512	31		SHA2-512

esp encrypt(Default: blowfish):***aes***

auth type(Default: md5):***md5***

apn: no process killed

Now you have new encrypt way: blowfish-md5, You must restart APN GW or

Restart apngw by : advconf apngw restart, to take it to work.

其中的数值，表示速度的参考。这是我们在标准的 100M 的网络环境中的测试值。以 NULL 为基数，其他的加密算法对速度的影响可参考该值。

说明：以上测试值仅供参考。在具体的实际应用中，由于网络状况的不同，使用的效果会有所不同。

第五章　工作站配置

本章介绍了如何设置局域网内的电脑。在以上的章节中，我们已经配置好了新 E 通。现在我们需要设置局域网之内的其他电脑。按照本章的配置之后，您可以让局域网内的电脑利用新 E 通进行 Internet 浏览、利用 VPN 通道访问其他远程的电脑。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

网络设置

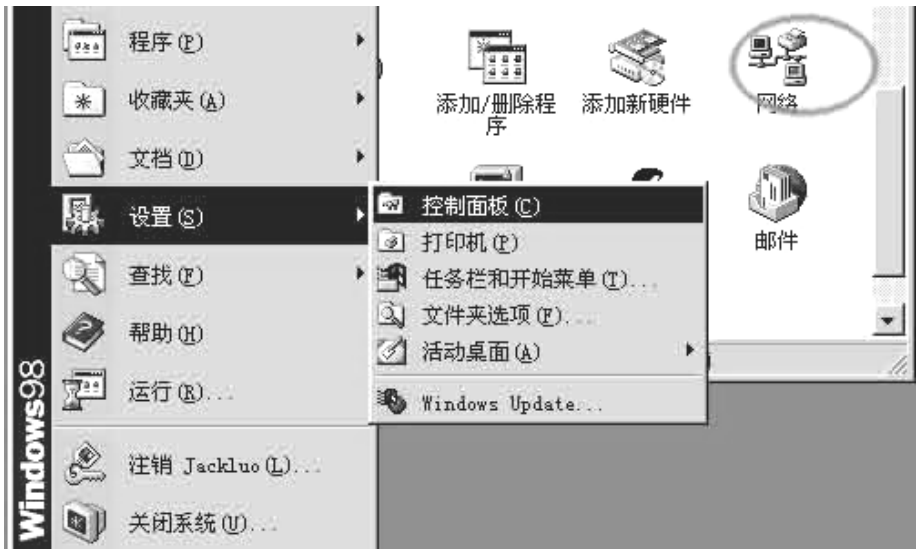
设定 TCP/IP 使用其 IP 与 APN GATEWAY 在同一个子网中。并且保证不用同一个 IP 地址，以确定不会发生网络冲突。并把 IP 的缺省网关指向新 E 通 GATEWAY。

举例说明：如新 E 通的 IP 地址是： 192.168.3.10, 子网掩码是：255.255.255.0, 那么其它工作站的 IP 可以是：192.168.3.1, 192.168.3.2, 或 192.168.3.11, 192.168.3.12 等等，但工作站的 IP 不得与新 E 通 GW 的 IP 一样。

注：这里的工作站指的是要上网的 WINDOWS98/NT 等。

WINDOWS 工作站设置举例

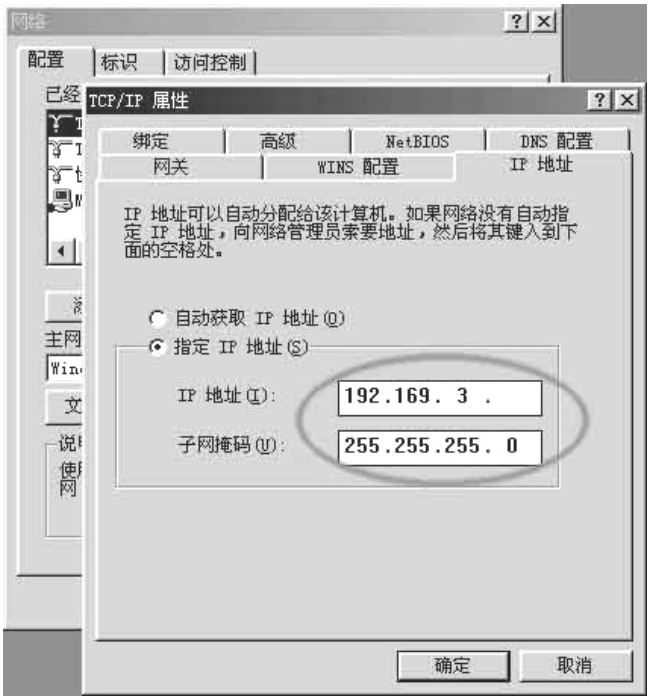
用鼠标点按 WINDOWS 桌面下方的[开始]，选取[设置]，[控制面板]，如下图：



用鼠标双击[网络]图标，出现有关网络配置的对话框，找出网卡对应的的 TCP/IP 对应的项并点按[属性]。如下图所示，如果这里没有网卡或 TCP/IP 选项，按下面的[添加]加入要应项。

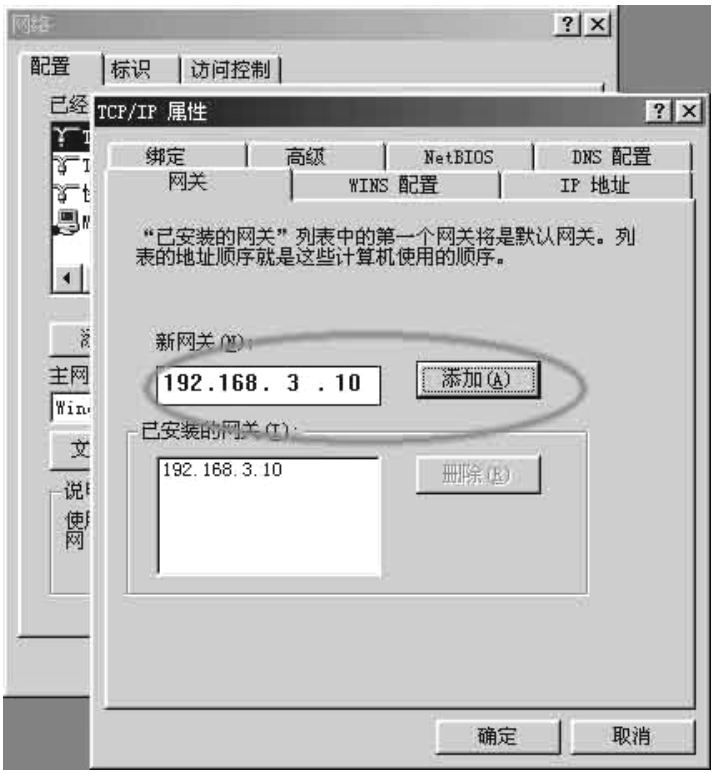
地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

点按属性后，出现如下的对话框，有其[IP 地址]中写入分配给这个工作站的 IP 地址，和子网掩码(子网掩码我们一般定为：255.255.255.0).



地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

转入[网关]，填入新 E 通的 IP 地址，并按[添中]，如下图：



转入[DNS 配置]，在“DNSAPN 搜索顺序”中添加本地 ISP 的 DNS 地址，在[主机]中填入工作站的名称，在[域]中填入内部域名的名称，在[域后缀搜索顺序]中写入本工作站的域名。如果您的新 E 通配置了 DNS 并已正常启动，此处也可输入新 E 通内部接口的 IP 地址。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

后请点击“确定”按钮以保存输入的数据。并按计算机给出的提示重新启动工作站。

重新启动后即可上网。工作站可以按正常使用上网的方式来使用互联网，也可以使用内部的虚拟网。

提示：以上所列范例是我们常用的 windows 98 中的设置，如果您用的是其他操作系统，例如 linux 或 unix，可参考以上所描述设置工作站的 ip 地址，子网掩码和网关。
如果您的新 E 通启动了 DHCP/DNS 服务，您可以采用自动获得 IP 地址的选项。这样网卡就不需要任何其他的设置。

第六章 防火墙设置

新 E 通产品具有强大的防火墙功能，能完成专用防火墙的绝大多数功能。如果您采用更高端的新 E 通产品，您还可以设置专业的 DMZ 区等，可以获得专业防火墙的功能。

关于网络安全的研究分析中，防火墙（Firewall）是被经常强调的重点，它基本功能是过滤并可能阻挡本地网络或者网络的某个部分与 Internet 之间的数据传送（数据包）。数据包其实就是一段段的数据，其中同时包括了用来把它们发送到各自的目的地所必须的信息。你可以把数据包想象成一个邮包：数据包本身就是邮包中的数据，而信封上则是所有用来把这些信息发送到正确的机器和正确的程序中去的书信抬头，它同时还包含着回信地址等方面的信息。在其具体的过滤工作过程中，防火墙将接管在此之前从网络内部存取 Internet 和从 Internet 存取该内部网络的路由设置。

我们的感觉是以前的防火墙专门用来过滤一些非法的数据包，要么为什么其中的一种类型称为包过滤型防火墙呢？发展到现在，它的功能是日益增多，不仅能够过滤数据包，还能够作网络地址转换，作代理等等。新 E 通防火墙功能就能完成这些工作，为您建立一个高效的安全网络环境。

设置基础

1. NAT 和 DNAT

NAT（Network Address Translation）即网络地址转换。即将内网的 IP 地址或者外网的 IP 地址转换，一般分为源地址转换 Source NAT（SNAT）和目的地址转换 Destination NAT （DNAT）。常见的包伪装（Masquerading）就是一个 SNAT 特例，主要用来将有限的 IP 地址动态或静态地与内部的 IP 地址对应起来，用来缓解地址空间短缺的问题。端口转发（Port forwarding）、负载分担、以及透明代理，都属于 DNAT，主要用于外网主机访问内网主机。
新 E 通支持 NAT 和 DNAT。同时内置了 NAT 代理上网和 DNAT 的端口转发。

2. 新 E 通防火墙功能的架构说明

系统分为两大模块。一个是对内部的分组管理，一个是防止外部的攻击。

设置概述

在[APNGW /]下输入 fwconf，可以进入防火墙的配置模式。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

[APNGW /]# ***fwconf***

APN GW Firewall (APN FW) Configuration

Copyright: Authcyber.com 2002-2016, All right reserved

Type help to list available command.

Type command to enter certain command's function menu.

FW>输入 help 可以看到所有的命令。

FW> ***help***

APN GW FIREWALL CONFIGURATION AND MANAGEMENT

```
==========================================================
lanuser      : Local User's Access filter
apnuser      : Share HOST or Service to this VDOMAIN user
group        : Self-defined service group for user
manual       : Manual Setting Firewall for more control
----------------------------------------------------------
admin        : WAN User Access APN GW for management
----------------------------------------------------------
nat          : SNAT DNAT Port forward management
----------------------------------------------------------
loaddefault: Restore to default setting
saveall      : Save All firewall configuration
----------------------------------------------------------
start        : Restart APN GW firewall
stop         : Stop All, and set policy to allow
----------------------------------------------------------
log          : Log Management
----------------------------------------------------------
exit         : Exit to terminal prompt
==========================================================
FW>
```

以上设置：

lanuser： 对局域网的用户上网的管理；

apnuser： 对 apn 用户的管理；

group： 建立组，定义组策略；

manual： 手工设置；

admin： 配置广域网用户对新 E 通的操作；

nat:： 对 NAT 进行配置；

loaddefault： 恢复缺省设置

saveall： 保存所有配置

start： 启动防火墙

stop： 停止防火墙

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

log：　　日志管理
exit：　　退出配置

对局域网用户的管理

在本组中，您将可以对局域网的用户上网进行配置，可以从协议、端口、MAC 地址等参数来配置防火墙。这项功能主要是用于对新 E 通所在的机器的局域网用户的上网代理功能进行限制和管理。

在[APNGW /]下输入 fwconf，可以进入防火墙的配置模式。

[APNGW /]# ***fwcon***
APN GW Firewall (APN FW)　Configuration
Copyright: Authcyber.com 2002-2016, All right reserved

Type help to list availabe command.
Type command to enter certain command's function menu.

FW> ***lanuser***　　＃进入 lanuser 配置模式
Config LAN user access
You can use : {config|active|save}

FW_lanuser>***config***
config
Note: If you have modify firewall rule by manual way,　This below process
　　will reset what you active new rules

press enter to continue....
POLICY: ACCEPT　　＃缺省策略为接受
==========
DROP IP list
==========
　　＃此处加入拒绝的策略
IP Address Range.
Format: <addr>[/mask] [group_name]
##　　|　　|　　\　Active Group, Omit means DROP
##　　|　　|　　{grouplist} for list have defined group
##　　|　　Netmask, Omit meas a unique host
##　May use IP addr or MAC format, NN:NN:NN:NN:NN:NN, N is hexadecimal
##　If use MAC Addr, not input mask at here. NOT support apnuser chain
##{append|insert|delete|policy} for switch input mode, exit to termnal
****
APPEND >***176.16.10.137***　　＃在 APPEND 状态下输入 IP 地址或 MAC 地址。
APPEND>***exit***　　＃退出编辑状态。
FW_lanuser> ***active***　　＃启用编辑过的规则。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

Active local user success.

FW_lanuser>

按照此方法，可以拒绝 176.16.10.137 这个地址的所有代理上网服务。

如果要对许多人设定同样的权限，就可以用分组管理的功能来实现。可以实现定义一个或多个组，每个组分配不同的规则，例如定义组 wwwusers，该组用户只能进行 www 浏览，不能做其他事情。关于如何定义组和相应的规则，下一节会详细的描述。

FW_lanuser> ***config***

POLICY: ACCEPT

==========

DROP IP list

==========

172.16.10.137@wwwusers　　#表示 172.16.10.137 这个地址应用 wwwusers 的策略

176.16.10.137@wwwusers　　#表示 172.16.10.137 这个地址应用 wwwusers 的策略

IP Address Range.

Format: <addr>[/mask] [group_name]

| | \ Active Group, Omit means DROP

| | {grouplist} for list have defined group

| Netmask, Omit meas a unique host

May use IP addr or MAC format, NN:NN:NN:NN:NN:NN, N is hexadecimal

If use MAC Addr, not input mask at here. NOT support apnuser chain

##{append|insert|delete|policy} for switch input mode, exit to termnal

****

APPEND > ***00:e0:4c:54:8d:e3 wwwusers***　#表示把这个 MAC 地址应用 wwwusers 的策

以上描述的是在 APPEND 状态下加入规则。同样有效的模式有：

模式	状态切换方式	说明
APPEND>	add	加入规则
DEL>	del	删除规则
POLICY>	policy	定义缺省策略，有效方式：accept drop

对新 E 通用户的管理

在本组中，您将可以对局域网的用户的安全进行配置。这项功能主要是用于对新 E 通所在的机器的局域网用户对于同一个虚拟域内的访问进行限制和管理。

在许多公司里，例如财务是一个单独的安全性要求很高的部门，如果建议虚拟专用网络，那就意味者同公司之间可以被互相访问。但是在 APNUSER 这个功能里面，可以设定对局域网的机器开放或不开放访问的的权限。换言之，这里是防止来自内部的安全隐患。

此处增加的地址，会按照设定的策略，让同一个新 E 通虚拟域内的其他电脑可以访问或不可以访问。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

FW> ***apnuser***
Config APN user access
You can use : {config|active|save}

FW_apnuser>***config***
Note: If you have modify firewall rule by manual way, This below process
will reset what you active new rules

press enter to continue....
POLICY: ACCEPT
==========
DROP IP list
==========

IP Address Range.
Format: <addr>[/mask] [group_name]
| | \ Active Group, Omit means DROP
| | {grouplist} for list have defined group
| Netmask, Omit meas a unique host
May use IP addr or MAC format, NN:NN:NN:NN:NN:NN, N is hexadecimal
If use MAC Addr, not input mask at here. NOT support apnuser chain
##{append|insert|delete|policy} for switch input mode, exit to termnal
****

APPEND >172.16.10.12 ＃此处加入的地址将不会被其他同域的机器访问注意缺省的策略是 ACCEPT，即为可以被访问。加入的地址是不可以被访问。

定义组策略

前面的设置之中，可以把某一些 IP 地址或 MAC 地址单独的应用不同的策略，这需要定义一些组和相应的策略。

FW> ***group***
Config self-defined chains, Define service group
Available command is: {list|show|new|edit|delete|active|
disactive|save }
<list>
FW_group>***list*** ＃列出已经定义的组名
Have Defined Group List
==========
mailusers [Actived]
<show>
FW_group> ***show*** #显示已有的组策略
Have Defined Group List
==========
mailuser [Actived]

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

Group name to show: ***popusers*** #输入需要显示的组策略

popusers

==========

:P ACCEPT

:A -j DROP -p tcp --dport pop-3

==========end===

<new>

FW_group> ***new*** #新建一个组

Group to create: ***wwwuser*** #输入组名字

POLICY NOT set yet

==========

ACCEPT Service

Format: <service_name|{tcp/icmp/udp}:port_num>

available: {www|dns|telnet|ftp|pop3|smtp|oicq|icq|} or

{tcp|udp|icmp|<proto_num>}:<port_Number>

##

##{add|de|policyl} for switch input mode, exit to break input

****

POLICY >***accept*** #输入缺省策略的方式

POLICY: ACCEPT

==========

DROP Service list

==========

DROP Service

Format: <service_name|{tcp/icmp/udp}:port_num>

available: {www|dns|telnet|ftp|pop3|smtp|oicq|icq|} or

{tcp|udp|icmp|<proto_num>}:<port_Number>

##

##{add|de|policyl} for switch input mode, exit to break input

****

ADD >

POLICY: ACCEPT

==========

DROP Service list # 缺省策略为 ACCEPT，以下的列表是拒绝的

==========

telnet

ftp

pop3

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

oicq

DROP Service
Format: <service_name|{tcp/icmp/udp}:port_num>
available: {www|dns|telnet|ftp|pop3|smtp|oicq|icq|} or
{tcp|udp|icmp|<proto_num>}:<port_Number>
##
##{add|de|policyl} for switch input mode, exit to break input
****

ADD > ***icq*** #此处加入需要限制（允许）的服务或端口

<delete>
Have Defined Group List
==========
demo [Actived]
wwwuser [Inactive]
wwwusers [Inactive]

Group to delete: ***demo*** #删除已经定义的组策略，
demo is referenced. #如果是已经激活的组，是不能删除的。
Disable the uesr who use it before delete or inactive it.

FW_group>
FW_group> disactive
Have Defined Group List
==========
demo [Actived]
wwwuser [Inactive]
wwwusers [Inactive]
Group to disactive: ***demo*** #可以单独的激活或不激活某一个特定的组

定义外网访问许可

这里设定外网是否可以访问新 E 通。这主要用于是否允许从外网地址 telnet 过来。如果您需要从远程公网上的电脑来配置或访问新 E 通，您需要设置许可。

FW> ***admin***
WAN User Access APN GW switch to yes or no
Available command is: {open |close|save}

FW_admin> ***help***
You can use : {open|close |save}

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

FW_admin> ***open*** # 设置可以从公网 telnet 到新 E 通。

FW_admin>***save***

Firewall Setting Saved.

open 是允许，close 是不允许，save 为保存设置。

NAT 设置

这里设定新 E 通的 NAT 功能。可以实现端口和协议的转发。

FW> ***nat***

NAT, Support DMZ if available

Available command is: {show|edit|active|disactive|save}

FW_nat> ***help***

Config self-defined chains, Define service nat

Available command is: {show|edit|active|disactive|save}

FW_nat> ***show*** #列出已经设置的 NAT 策略

DNAT

==========

:A -p tcp --dport 1720 --to-destination 176.16.10.88:1720

:A -p udp --dport 4998 --to-destination 176.16.10.88:4998

:A -p udp --dport 4999 --to-destination 176.16.10.88:4999

:A -p udp --dport 5000 --to-destination 176.16.10.88:5000

:A -p udp --dport 5001 --to-destination 176.16.10.88:5001

==========end===

FW_nat>***edit*** #进入编辑模式设置 NAT 策略

DNAT: Port forward

==========

tcp:1720->176.16.10.88:1720

udp:4998->176.16.10.88:4998

udp:4999->176.16.10.88:4999

udp:5000->176.16.10.88:5000

udp:5001->176.16.10.88:5001

Format: service_name|{tcp|udp}:port_num->dest_ip[:port[-port]]

available: {www|telnet|ftp|pop3|smtp} or

{tcp|udp}:<port_Number>

eg1, telnet->192.168.32.250

eg1, tcp:8080->192.168.32.240:80

##{add|del} for switch input mode, exit to break input

****

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

ADD >

选择配置后，缺省是 ADD 方式。这里只有两种方式：

ADD> 增加一条转发配置，用 add 可以切换到此方式；

DELETE > 删除一台转发配置，用 del 可以前后到此方式。

在 ADD 方式下，您可以加入您需要转发的目的地址和端口。系统提供了 www/telnet/ftp/pop3/smtp/作为标准的端口。您可以输入名字而无需输入端口号。例如，此时新 E 通的公网地址是 202.96.134.123，我们需要把该地址作为 WEB 服务。但是提供 WEB 服务的服务器在内网里面，其 IP 地址是 192.168.32.250。您需要如下设置：

ADD >***www->192.168.32.250***

DNAT: Port forward

==========

www->192.168.32.250

Format: service_name|{tcp|udp}:port_num->dest_ip[:port[-port]]

available: {www|telnet|ftp|pop3|smtp} or

{tcp|udp}:<port_Number>

eg1, telnet->192.168.32.250

eg1, tcp:8080->192.168.32.240:80

##{add|del} for switch input mode, exit to break input

****

ADD >***exit*** 配置完毕需要退出配置模式。

CONF_portfwd>***start*** 开始此项服务

CONF_portfwd>***save*** 把所做的设置存盘。

如果您需要删除以上配置，您只需要在上面的 ADD 方式下输入 **del** 后转换到 ADD>del 方式后采用同样的配置。

注意：在配置 NAT 之后，您需要先 start 此项服务之后，再 save。因为 save 不光是保存了您的配置，还把您是否启动该项服务的状态也保存了下来。

恢复缺省设置

这里可以恢复到出厂的设置

FW>***loaddefault***

This will destroy all you defined firewall rules, and restore to

default setting

NOTE: NAT and Sef-defined group not set to default, You must set

it manual if need

Are you sure to restory to default firewall setting (y/n)?***y***

这样可以恢复到缺省的设置。

日志

FW> ***log***

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

```
Logs Management
You can use : {read | tail }
FW_log> tail                                    # 查看最新的日志文件
Feb  2 20:19:03 GW2 daemon.notice pppd[1134]: Connection terminated.
Feb  2 20:19:07 GW2 daemon.err pppoe[1135]: Timeout waiting for PADO packets
Feb  2 20:19:07 GW2 daemon.info pppd[1134]: Exit.
Feb  2 20:19:07 GW2 daemon.notice pppd[1136]: pppd 2.4.1 started by root, uid 0
Feb  2 20:19:07 GW2 daemon.info pppd[1136]: Using interface ppp0
Feb  2 20:19:07 GW2 daemon.info pppd[1136]: Connect: ppp0 -> /dev/ttyp0
Feb  2 20:19:38 GW2 daemon.warn pppd[1136]: LCP: timeout sending Config-Requests
Feb  2 20:19:38 GW2 daemon.notice pppd[1136]: Connection terminated.
Feb  2 20:19:42 GW2 daemon.err pppoe[1137]: Timeout waiting for PADO packets
Feb  2 20:19:42 GW2 daemon.info pppd[1136]: Exit.
Feb  2 20:19:42 GW2 daemon.notice pppd[1138]: pppd 2.4.1 started by root, uid 0
Feb  2 20:19:42 GW2 daemon.info pppd[1138]: Using interface ppp0
Feb  2 20:19:42 GW2 daemon.info pppd[1138]: Connect: ppp0 -> /dev/ttyp0
Feb  2 20:20:13 GW2 daemon.warn pppd[1138]: LCP: timeout sending Config-Requests
Feb  2 20:20:13 GW2 daemon.notice pppd[1138]: Connection terminated.
Feb  2 20:20:17 GW2 daemon.err pppoe[1139]: Timeout waiting for PADO packets
Feb  2 20:20:17 GW2 daemon.info pppd[1138]: Exit.
Feb  2 20:20:17 GW2 daemon.notice pppd[1140]: pppd 2.4.1 started by root, uid 0
Feb  2 20:20:17 GW2 daemon.info pppd[1140]: Using interface ppp0
Feb  2 20:20:17 GW2 daemon.info pppd[1140]: Connect: ppp0 -> /dev/ttyp0
FW_log>read                                     #查看所有日志文件
```

第七章 路由设置

本章描述了新 E 通的路由设置。一般情况下，新 E 通工作之后，会自动获得 VPN 通道的路由。但如果您还需要配置其他的路由，可参考本章所描述进行设置。

新 E 通产品具有强大的路由功能，您可以定制自己的路由。

注意： 当您完成 setup 中的设置时，系统已经具备路由功能。本章目的在于提供给高级用户为了完成某些特定的功能而手动修改路由。例如您在一端的局域网内有两个不同的网段而且都需要通过新 E 通上网，您就需要手工加入其中一个与新 E 通的 Eth0 不在同一网段的路由。

查看当前路由表

您可以使用以下命令查看当前的路由表信息。

APNGW# ***route***

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

系统会出现以下信息：

[APNGW /]# route

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
218.17.65.1	*	255.255.255.255	UH	0	0	0	ppp0
176.16.10.1	*	255.255.255.255	UH	0	0	0	eth0
172.31.250.250	*	255.255.255.255	UH	0	0	0	eth1
172.31.250.0	*	255.255.255.0	U	0	0	0	eth1
192.168.20.0	202.60.239.129	255.255.255.0	UG	0	0	0	tunl0
176.16.10.0	*	255.255.255.0	U	0	0	0	eth0
176.16.10.0	*	255.255.255.0	U	0	0	0	tunl0
192.168.0.0	211.162.110.241	255.255.255.0	UG	0	0	0	tunl0
192.168.30.0	218.17.79.159	255.255.255.0	UG	0	0	0	tunl0
192.168.40.0	202.60.249.134	255.255.255.0	UG	0	0	0	tunl0
localnet	*	255.0.0.0	U	0	0	0	lo
default	218.17.65.1	0.0.0.0	UG	0	0	0	ppp0
default	*	0.0.0.0	U	0	0	0	tunl0

[APNGW /]#…….

以上信息会因为新 E 通的设置的不同而不同。具体内容请用户查看自己系统的显示。

配置概述

新 E 通的路由配置也是在高级配置模式下进行的。使用 root 登录，在提示符 APNGW#下键入：

APNGW# ***advconf***

CONF>***route***

Route config menu, available command is {edit|list|start|stop|save|exit}

CONF_telnet>***edit***

In Most Time, You need not this function, but if you have more than one subnet want to connect to internet by APN or have an complex network topology, you may use this function.

Use ae to edit your manual route table.

Use ctrl_w to save the change, Use ctrl_c to exit.

您手工增加的路由会保存在一个配置文件里。您此时按任意键可以编辑该文件。如果您需要保存该文件，按下 ctrl＋w，退出按 ctrl＋c。关于这个文件的书写格式，您可以参考以下的小节：手工设置路由。

注意，这里的配置文件保存仍然是保存在 RAM 中的。如果您要保存到系统中，您还需要在 CONF_route 下用 **save** 命令。

说明： route 支持以下几个命令：edit , list , start, stop, save, exit。其含义如下：

edit： 手工配置路由；

list： 列出您已经配置的路由；

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

start：启动您设置的路由；

stop：停止您设置的路由；

save： 把配置保存起来。如果您不保存，那么下次启动时会丢失本次配置。

exit：退出配置模式。

手工设置路由

请先阅读上一小节。本小节所述，需要加在上一小节中所提及的配置文件中。即用 edit 命令之后，会出现一个编辑的界面。您需要把您要作的路由设置放在其中。

命令格式：

route
[-v] [-A family]add(or del) [-net|host] target [netmask Nm] [gw GW] [metric N][mss M][window W]
[irtt I][reject][mod][dyn][reinstate][[dev] If]

一般情况下许多参数我们都用不到。下面取一典型的路由设置：

route add –net 192.168.0.0 mask 255.255.255.0 dev eth0

通过 eth0 加一个 192.168.0.x 这个网段的的路由。

第八章 管理新 E 通

本章主要讲述了如何管理新 E 通。在本章中所提及的部分命令，其他前面的章节可能已经提及或详细的描述过。但作为对新 E 通管理的所有命令的汇总，仍然将描述这些命令。

查看所有连接

查看当前有哪些新 E 通连接，可用 route 命令。该命令可以列出与当前新 E 通相连的其他新 E 通的公网地址。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

但其中自己显示为 default 的一个是本机局方 IP。

```
APNGW# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
218.17.65.1     *               255.255.255.255 UH    0      0        0 ppp0
176.16.10.1     *               255.255.255.255 UH    0      0        0 eth0
172.31.250.250  *               255.255.255.255 UH    0      0        0 eth1
172.31.250.0    *               255.255.255.0   U     0      0        0 eth1
192.168.20.0    202.60.248.73   255.255.255.0   UG    0      0        0 tunl0
176.16.10.0     *               255.255.255.0   U     0      0        0 eth0
176.16.10.0     *               255.255.255.0   U     0      0        0 tunl0
192.168.0.0     211.162.110.241 255.255.255.0   UG    0      0        0 tunl0
192.168.30.0    61.141.77.133   255.255.255.0   UG    0      0        0 tunl0
192.168.40.0    203.169.176.131 255.255.255.0   UG    0      0        0 tunl0
localnet        *               255.0.0.0       U     0      0        0 lo
default         218.17.65.1     0.0.0.0         UG    0      0        0 ppp0
default         *               0.0.0.0         U     0      0        0 tunl0
APNGW#
```

查看当前网络配置

在[APNGW/]下输入 ifconfig，您会看到当前的网络设置。

系统会出现以下类似的信息：

[APN GW/]***ifconfig***

```
lo      Link encap:Local Loopback
        inet addr:127.0.1    Mask:255.0.0.0
        UP LOOPBACK RUNING MTU:3924 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        Collisions:0
eth0    link encap:Ethernet HWaddr 00:E0:4C:67:03:4C
        inet addr:192.168.1.1 Bcast:192.168.1.255 Mask: 255.255.255.0
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        Collisions:0
        Interupt:15 Base address:0xe000
eth1    link encap:Ethernet HWaddr 00:E0:4C:67:03:4C
        inet addr:172.31.250.250    Bcast:172.31.250.255 Mask: 255.255.255.0
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        Collisions:0
        Interupt:15 Base address:0xe400
ppp0    Link encap:Point-to-Point Protocol
```


地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

inet addr:218.17.66.216 P-t-P:218.17.65.1 Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1492 Metric:1
RX packets:19301 errors:0 dropped:0 overruns:0 frame:0
TX packets:20049 errors:0 dropped:0 overruns:0 carrier:0
collisions:0

其中的含义：

lo 为 loopback 设备；

eth0 和 eth1 分别为两个网络接口卡；

如果此时连接到 Internet，还会有一个设备为 ppp0。同时也会显示它的 ip 地址。如果您需要查询拨号或虚拟拨号时新 E 通连接到 intenet 时公网的 IP 地址，那么可用 ifconfig 命令，其中的 ppp0 就是该地址。

检测广域网连接

如何知道新 E 通是否已经连接到 internet？同所有的系统一样，新 E 通也提供 Ping 命令。您可以使用以下简单的方法检测是否已连接。

ping *ipaddress*

其中的 ip 地址是指您所知道的 internet 的存在的 ip 地址。例如 202.96.134.133。如果成功返回，就表示已经连接到 internet。

ping 202.96.134.133

PING 202.96.134.133(202.96.134.133):56 data bytes
64 bytes from 202.96.134.133: icmp_sq=0 ttl=225 time=120 ms
64 bytes from 202.96.134.133: icmp_sq=0 ttl=225 time=110 ms
…….
Ping 包被成功返回：网络已通。

ping 192.168.100.100

无成功返回信息，按 ctrl＋c 退出，显示：
30 packets transmitted, 0 packets received, 100% packet loss
Ping 包返回失败：网络不通或对方 IP 拒绝 ping 包。

如果您使用的是 adsl，您可以使用 adsl-status 查看当前的网络情况。

[APNGW /]# **adsl-status**
adsl-status: Link is up and running on interface ppp0
ppp0 Link encap:Point-to-Point Protocol
inet addr:218.17.66.216 P-t-P:218.17.65.1 Mask:255.255.255.255
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1492 Metric:1
RX packets:19301 errors:0 dropped:0 overruns:0 frame:0
TX packets:20049 errors:0 dropped:0 overruns:0 carrier:0
collisions:0

检测局域网连接

同样的方法，您可以使用 ping 您的局域网地址查看局域网的连接是否成功。在检测之前，建议先检测新 E 通本身的 eth0 是否已经 up。方法如下：

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

假设您已设置 APN 的 eth0 的 ip 是 192.168.0.1。而您在局域网内有一台计算机的 ip 地址是 192.168.0.10。您可以键入以下命令：

ping 192.168.0.1

PING 192.168.0.1(192.168.0.1):56 data bytes

64 bytes from 192.168.0.1: icmp_sq=0 ttl=225 time=120 ms

64 bytes from 192.168.0.1: icmp_sq=0 ttl=225 time=110 ms

…….

按 ctrl＋c 中止检测。此项表示 eth0 的设置已经成功。

ping 192.168.0.10

无成功返回信息

按 ctrl＋c 中止检测。显示

50 packets transmitted, 0 packets received, 100% packet loss

此项表示局域网的连接已经成功。

ping 命令详解

ping 命令用于查看网络上的主机是否在工作，它向该主机发送 ICMP ECHO_REQUEST 包。有时我们想从网络上的某台主机上下载文件，可是又不知道那台主机是否开着，就需要使用 ping 命令查看。

该命令的一般格式为：

ping [选项] 主机名/IP 地址

命令中各选项的含义如下：

-c 数目 在发送指定数目的包后停止。

-d 设定 SO_DEBUG 的选项。

-f 大量且快速地送网络封包给一台机器，看它的回应。

-I 秒数 设定间隔几秒送一个网络封包给一台机器，预设值是一秒送一次。

-l 次数 在指定次数内，以最快的方式送封包数据到指定机器(只有超级用户可以使用此选项)。

-q 不显示任何传送封包的信息，只显示最后的结果。

-r 不经由网关而直接送封包到一台机器，通常是查看本机的网络接口是否有问题。

-s 字节数 指定发送的数据字节数，预设值是 56，加上 8 字节的 ICMP 头，一共是 64ICMP 数据字节。

账号管理

新 E 通的高级配置中，可以配置账号。您可以在这里增加新的账号或更改删除账号，或更改密码：

[APNGW /]#**advconf**

CONF>**user**

User Mangement,available command is :{add|del|list|passwd|save}

改变登录密码

CONF_usr>**passwd**

IF YOU ARE GONIGN TO CHANGE ROOT PASSWD, BE SURE REMEMBER YOUR ROOT PASSWORD.IF YOU LOSS IT AND YOU WILL NEVER LOGIN APN GW AGAIN

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

Press a key to continue….

User Name: **root**

Enter the new password(minimum of 5,maximum of 8 characters)

Please use a combination of upper and lower case letter and numbers.

Enter new password:*****

Re-enter new password:*****

Password changed.

增加一个用户

CONF_usr>**add**

New User Name: **guest**

Change the password for guest

Enter the new password(minimum of 5,maximum of 8 characters)

Please use a combination of upper and lower case letter and numbers.

Enter new password:*****

Re-enter new password:*****

Password changed.

口令

许多人都把所有的东西保存在计算机上，防止别人查看这些信息的方法就是用口令把计算机保护起来。没有什么东西是绝对安全的。与常识相反的是：无法破解的口令是不存在的。只要给足时间和资源，所有的口令都能用社会工程（原文是 social engineering，找不出更好的翻译，大致的意思是用社会和心理学的知识，而不是用纯粹的技术手段）或强行计算的方法猜出来。

通过社会工程或其它方法获得服务器的口令是最简单和最流行的入侵服务器的方法。决大多数的技术支持人员很容易获得其他用户的口令，因为用户的安全意识很差而且很轻易就相信自己的同事，特别是帮助自己解决问题的人。有很多登记在案的成功入侵就是因为一些别有用心的人利用安全管理上的松懈而获得成功的。有时候，在特定的时间在特定的地点，上级或老板对员工喊话就有可能泄露机密，导致可怕的后果。

因为破解口令是一项很耗时间和资源的工作，所以应该使得口令文件难于破解，这样即使黑客获取了口令文件也不能轻易破解。要有一个好的口令检查机制，在用户选择新口令或改变旧口令的时候，来排除那些有安全隐患的口令。那些字典里的单词、或者全是大写或全是小写的以及没有包含数字或特殊字符的字符串是不能用来做口令的。建议用下面的规则选择有效的口令：

* 口令至少要有 6 个字符，最好包含一个以上的数字或特殊字符。
* 口令不能太简单，所谓的简单就是很容易猜出来，也就是用自己的名字，电话号码、生日、职业或者其它个人信息作为口令。
* 口令必须是有有效期的，在一段时间之后就要更换口令。
* 口令在这种情况下必须作废或者重新设定：如果发现有人试图猜测你的口令，而且已经试过很多次了。

忘记口令

如果您不巧忘记了自己的口令，新 E 通提供一个 Rescue Mode，可以不用口令登录。这需要使用者直接接触到新 E 通，通过其配置的 console 线来恢复口令。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

在用控制台进入新 E 通配置之中，其中会有一个信息：

Press R with 3 seconds enter rescue mode. Configuring and Starting LAN Network.....

这时候会有一个 3 秒的时间您可以通过按 R 键登录新 E 通而不需要输入口令。登录之后，您可以更改您的口令或增加新的用户名和口令。

警告：

如果您改变了您的 root 密码而不巧将其忘记的话，您可以使用安全模式进入。该模式不可以远程操作。

安全性详述

系统的安全性概述

广域网和局域网分别有不同的物理接口。中间是通过防火墙来做转换。一般的系统都是通过这种方式连接到 Internet 的。新 E 通产品自带防火墙功能，如果需要，也可以考虑另外增加第三方的防火墙产品。

安全隐患可能来自内部和外部。目前的企业局域网基本上都采用以太网构架，访问机制为具有冲突检测的载波监听多路访问（CSMA/CD）方法。对于这种总线型以太网，黑客只要接入以太网上的任一节点进行侦听，就可以捕获发生在这个网上的所有数据包，这是以太网固有的安全隐患。对于内部的安全，一般可以采用网络分段的方式和采用局域网内加密网卡来解决；这并不在新 E 通讨论的范畴。而组建一个广域的虚拟专用网络之后，对于来之同一虚拟网络的异地机器的访问，新 E 通的防火墙也可以作到限制。

网络系统内各局域网边界的安全，可使用防火墙的访问控制功能来完成。同时，新 E 通支持多网段划分，可同时实现局域网内部各网段的隔离与相互的访问控制。

网络与其它网络如因特网互连的安全,可使用防火墙来实现二者的隔离与访问控制。同时，建议网络系统的重要主机或服务器的地址使用 Internet 保留地址，并有统一的地址和域名分配办法，这样一方面解决合法 IP 不足的问题，另一方面，利用 Internet 无法对保留地址进行路由的特点，杜绝与 Internet 直接互连。

网络系统内部各局域网之间信息传输的安全，可通过使用新 E 通的基于 IPSec 的 VPN 功能来实现信息的机密性与完整性保护。

网络地址转换是新 E 通的标准配置，从最简单的新 E 通的版本，都加入了该功能。 而基于 2.4Kernel 的防火墙 2.0,般采用双向 NAT：SNAT 和 DNAT。SNAT 用于对内部网络地址进行转换，对外部网络隐藏起内部网络的结构，使得对内部的攻击更加困难；并可以节省 IP 资源，有利于降低成本。DNAT 主要实现用于外网主机对内网和 DMZ 区主机的访问。

移动用户的接入安全问题。使用新 E 通提供移动用户的一次性口令认证机制，可以实现对移动用户的强身份鉴别。移动用户采用基于 PPTP 的客户端软件接入，其传输过程提供 128 位加密。

新 E 通主要采用五项技术来保证安全，分别是新 E 通架构（APN GW Architecture）、隧道技术（Tunneling）、加解密技术（Encryption & Decryption）、密钥管理技术（Key Management）、使用者与设备身份认证技术（Authentication）。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

新 E 通架构

为本公司的新 E 通建立更快更迅速的连接。
新 E 通体系安全可以归结如下：

- 全部基于开发源码的 Linux 设计；
- 身份验证功能，鉴定新 E 通的合法性；
- 多种加密算法支持；
- 提供强大的防火墙功能；
- 新 E 通架构提供良好的扩展性，可以任意节点的可扩展性；

隧道技术

隧道技术是 VPN 的基本技术类似于点对点连接技术，它在公用网建立一条数据通道（隧道），让数据包通过这条隧道传输。隧道是由隧道协议形成的，分为第二、三层隧道协议。第二层隧道协议是先把各种网络协议封装到 PPP 中，再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有 L2F、PPTP、L2TP 等。L2TP 协议是目前 IETF 的标准，由 IETF 融合 PPTP 与 L2F 而形成。

第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。第三层隧道协议有 VTP、IPSec 等。IPSec（IP Security）是由一组 RFC 文档组成，定义了一个系统来提供安全协议选择、安全算法，确定服务所使用密钥等服务，从而在 IP 层提供安全保障。

新 E 通产品都是采用第三层的网络协议，支持 IPSec 和 GRE 两种协议。

加解密技术

加解密技术是数据通信中一项较成熟的技术，VPN 可直接利用现有技术。

- 验证握手使用 RSA 2048 位 加密技术；
- 数据传输使用 3DES 168 位、AES、BLOWFISH 等多种加密算法；
- 基于源和目的的 IP 地址通过互联网建立 IPSec 加密隧道
- MD5 数据摘要算法，保护数据传输的完整性
- 支持国家密码委员会推荐的加密算法。可选配国密办允许使用的加密卡（北京华正天网公司的 SJW 16 加密卡）
- 硬件加密速度：有三种方式可供选择，31M，签名 13 次/秒 或 50M，签名 13 次/秒 或 50M，签名 60 次/秒。
- 硬件加密卡密钥长度：对称：128 位，非对称：1024/2048 位；

使用者与设备身份认证技术：

使用者与设备身份认证技术最常用的是使用者名称与密码或卡片式认证等方式。

- 新 E 通与新 E 通之间的是相互认证的；支持 Pre-share Key 方式和 RSA2048 位硬件 key 的方式；

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

- 移动用户的身份由新 E 通产品来认证；
- 每个新 E 通设备需要合法的 Licenses。

新 E 通的 IPSec 架构

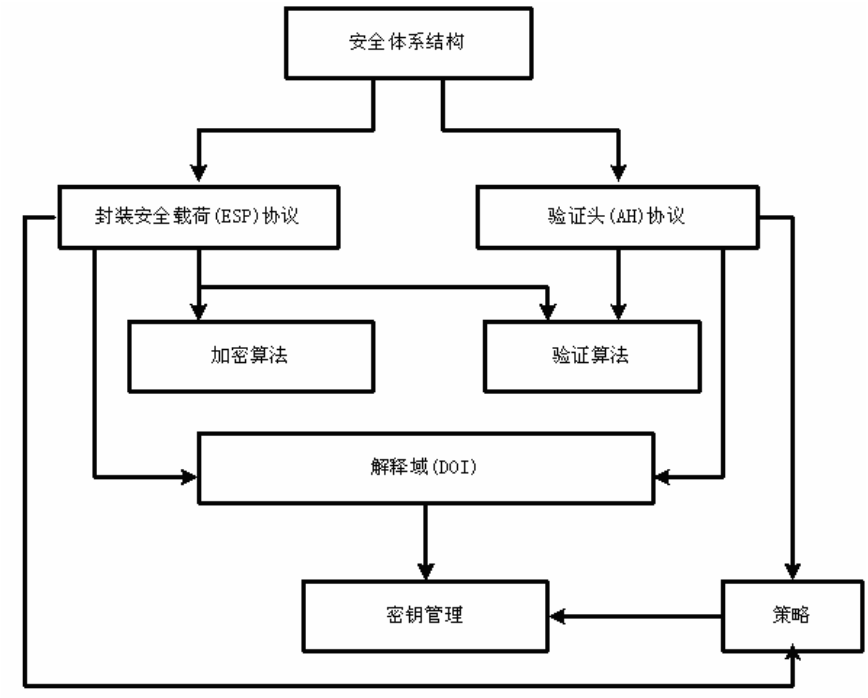
IPSec 是 IETF（因特网工程任务组）于 1998 年 11 月公布的 IP 安全标准。其目标是为 IPv4 和 IPv6 提供具有较强的互操作能力、高质量和基于密码的安全。IPSec 对于 IPv4 是可选的，对于 IPv6 是强制性的。

IPSec 在 IP 层上对数据包进行高强度的安全处理，提供数据源地验证、无连接数据完整性、数据机密性、抗重播和有限业务流机密性等安全服务。各种应用程序可以享用 IP 层提供的安全服务和密钥管理，而不必设计和实现自己的安全机制，因此减少密钥协商的开销，也降低了产生安全漏洞的可能性。IPSec 可连续或递归应用，在路由器、防火墙、主机和通信链路上配置，实现端到端安全、虚拟专用网络（VPN）和安全隧道技术。

IPSec 规范中包含大量的文档。其中最重要的是在 1998 年 11 月发布的，它们是 RFC2401、2402、2406 和 2408：

- RFC2401：安全体系结构概述；
- RFC2402：包身份验证扩展到 IPv4 和 IPv6 的描述；
- RFC2406：包加密扩展到 IPv4 和 IPv6 的描述;
- RFC2408：密钥管理能力规范。

对于这些特征的支持，IPv6 是强制性的， IPv4 为可选的。在这两种情况下，安全特征作为扩展报头实现，它跟在主 IP 报头后面。身份验证的扩展报头称作身份验证报头（AH 头），加密报头称 ESP(封装安全性有效载荷)报头。IPSec 安全体系结构如图所示：



- 安全体系结构：包含了一般的概念、安全需求、定义和定义 IPSec 的技术机制；
- 封装安全有效载荷（ESP）：覆盖了为了包加密（可选身份验证）与 ESP 的使用相关的包格式和常规问题；
- 验证头（AH）：包含使用 AH 进行包身份验证相关的包格式和一般问题；
- 加密算法：描述各种加密算法如何用于 ESP 中；

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

- 验证算法：描述各种身份验证算法如何用于 AH 中和 ESP 身份验证选项；
- 密钥管理：密钥管理的一组方案，其中 IKE（Internet 密钥交换协议）是默认的密钥自动交换协议；
- 解释域：彼此相关各部分的标识符及运作参数；
- 策略：决定两个实体之间能否通信，以及如何进行通信。策略的核心由三部分组成：SA、SAD、SPD。SA（安全关联）表示了策略实施的具体细节，包括源 / 目的地址、应用协议、Spi（安全策略索引）、所用算法 / 密钥 / 长度；SAD 为进入和外出包处理维持一个活动的 SA 列表；SPD 决定了整个 VPN 的安全需求。策略部分是唯一尚未成为标准的组件。

加密机制

密码函数可用来作为加密、解密、数据完整性、鉴别交换、口令存储与检验等等的一部分，借以达到保密、完整性和鉴别的目的。用于机密性的加密把敏感数据（即受保护的数据）变换成敏感性较弱的形式。当用于完整性或鉴别时，密码技术被用来计算不可伪造的函数。

加密算法可以是可逆的，也可以是不可逆的。

可逆加密算法有两大类：对称（即秘密密钥）加密。对于这种加密，知道了加密密钥也就意味着知道了解密密钥，反之亦然。 非对称（例如公开密钥）加密。对于这种加密，知道了加密密钥并不意味着也知道解密密钥，反之亦然。这种系统的这样两个密钥有时称之为“公钥”与“私钥”。

不可逆加密算法可以使用密钥，也可以不使用。若使用密钥，密钥可以是公开的，也可以是秘密的。

加密开始时，在明文上实施以产生密文；解密的结果或是明文，或是在某种掩护下的密文。使用明文作通用的处理在计算上是可行的，它的语义内容是可以理解的。除了以特定的方式（例如本原解密或恰切匹配），在计算上是不能处理密文的，它的语义内容已隐藏起来。有时故意让加密是不可逆的（例如截短或数据丢失），这时不希望导出原来的明文，例如口令。

密码函数使用密码变量，并作用于字段、数据单元或数据单元流上。两个密码变量为：

密钥，它指导具体的变换。密钥通常必须处于机密性状态，而且加密函数与初始变量可能加大延迟和提高带宽消耗。这使得把“透明的”和“可选的”密码技术加到现存系统中去变得复杂了。

初始变量，为了保持密文外表的随机性在某些密码协议中需要它。不论对于加密或解密而言，密码变量可以是对称的，或非对称的。

用在非对称算法中的密钥在数学上是相关的，一个密钥不能从另一个计算出来。这种算法有时称为公开密钥算法，这是因为可使一个密钥公之于众而另一个保持秘密。

当不知道密钥也能在计算上恢复明文时，密文可受到密码分析。如果使用一个脆弱的或是有缺陷的密码函数就会发生这种攻击。

窃听和通信业务流分析可能导致对密码系统的攻击，包括消息和字段的插入、删除与更改，先前有效密文的播放，以及冒充。所以密码协议的设计要抗攻击，有时还要抗通信业务流分析。对付通信业务流分析的一种具体办法

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

即“通信业务流机密性”，目的是掩蔽数据及其特征的出现或不出现。

如果密文被中继，那么在中继站和网关上地址必须是明文。如果数据只在每个链路上是加密的，而在中继内或网关内被解密(因而易受攻击)，这种体系称为用的是“链路加密”。如果只有地址(及类似的控制数据)在中继或网关内是明文，这种体系称为“端到端加密”。从安全观点看来更希望有端到端加密，但在体系结构上带来相当大的复杂性，特别是如果包含有频带内电子密钥分配(一种密钥管理功能)，更是如此。链路加密与端到端加密可以联合起来使用以达到多种安全目标。

硬件加密过程

- 硬件加密卡指标
  - 对称密码：密钥长度：128bit；加密速度：60Mbps。
  - 公开密钥密码：RSA：密钥长度：1024bit；处理速度：20 次/秒。
  - 椭圆曲线：密钥长度：160bit；处理速度: 约 100 次/秒。
  - HASH 算法：处理速度：60Mbps。
  - 密码卡处理速度：AT 总线：2Mbps，PCI 总线：20-30Mbps。
- 加密原理：

在源主机平台，析出的、被传送数据的 IP 包，在向网络接口传递之前，通过 SJW16 密码卡加密，然后再传送。被加密的数据，传输至目的主机平台的网络接口之后，先通过 SJW16 密码卡解密，然后再向上层传递。这样，在两个相互通信的主机平台之间传输的信息，都是经过 SJW16 密码卡加密的，而且对应用透明。

新 E 通 Firewall 2.0 基于 IPtables 的防火墙：

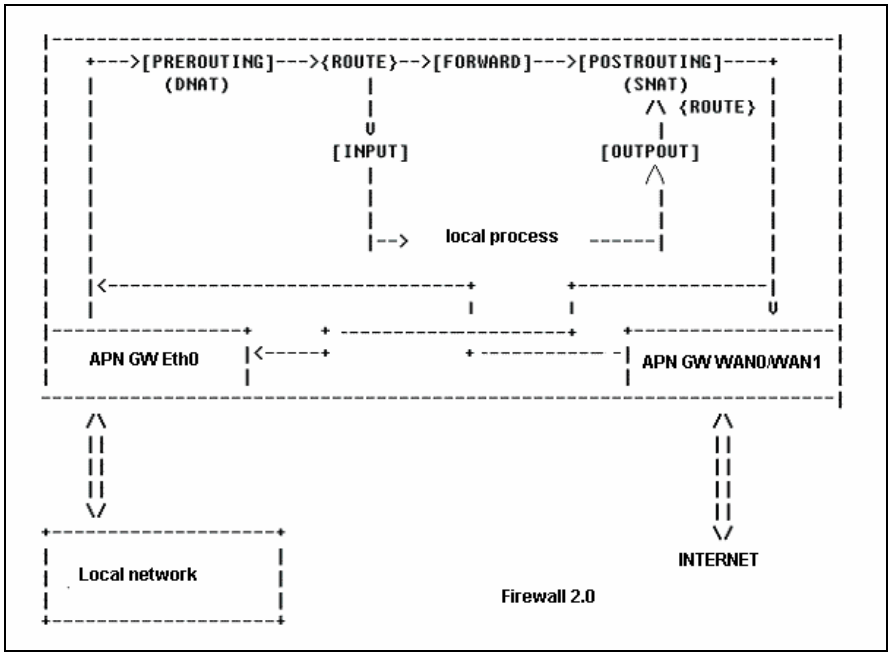
新 E 通 Firewall 2.0 是基于 Netfilter 架构的 IPtables 基础上建立起来的。由于结构的改变，比 1.0 有更多改进。例如支持 MAC 地址绑定和日志服务器和 DMZ 区等。

Netfilter 比以前任何一版 Linux 内核的防火墙子系统都要完善强大。Netfilter 提供了一个抽象、通用化的框架，该框架定义的一个子功能的实现就是包过滤子系统。Netfilter 框架包含以下三部分：

- 为每种网络协议(IPv4、IPv6 等)定义一套钩子函数（IPv4 定义了 5 个钩子函数),这些钩子函数在数据报流过协议栈的几个关键点被调用。在这几个点中，协议栈将把数据报及钩子函数标号作为参数调用 Netfilter 框架。
- 内核的任何模块可以对每种协议的一个或多个钩子进行注册，实现挂接，这样当某个数据包被传递给 Netfilter 框架时，内核能检测是否有任何模块对该协议和钩子函数进行了注册。若注册了，则调用该模块的注册时使用的回调函数，这样这些模块就有机会检查(可能还会修改)该数据包、丢弃该数据包及指示 Netfilter 将该数据包传入用户空间的队列。
- 那些排队的数据包是被传递给用户空间的异步地进行处理。一个用户进程能检查数据包，修改数据包，甚至可以重新将该数据包通过离开内核的同一个钩子函数中注入到内核中。

所有的包过滤/NAT 等等都基于该框架。内核网络代码中不再有到处都是的、混乱的修改数据包的代码了。当前 Netfilter 框架在 IPv4、IPv6 及 Decnet 网络栈中被实现。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029



防火墙的分组管理功能：

新 E 通 Firewall 2.0 支持防火墙的分组管理。简单的说，新 E 通提供了网络的具体的功能管理。可以把每个具有的策略分成组（group），对每个组都提供具体的防火墙策略。例如：定制销售部不能使用聊天软件；定制研发部可以有最大权限访问 Internet。

新 E 通防火墙的特点：

一般的 VPN 产品，如果组建一个虚拟专网之后，对内部的机器之间的访问是没有限制的。但是新 E 通架构的 VPN 产品，可以还在内部设置一个防范规则。

简单的说，对于来自内部的 VPN 网络的机器的访问，也需要通过授权才可以访问。新 E 通防火墙功能分为以下几部分：

lanuser： 对局域网的用户上网的管理；

apnuser： 对新 E 通用户的管理；

group： 建立组，定义组策略；

manual： 手工设置；

admin： 配置广域网用户对新 E 通的操作；

nat:： 对 NAT 进行配置；

loaddefault： 恢复缺省设置

saveall： 保存所有配置

start： 启动防火墙

stop： 停止防火墙

log： 日志管理

exit： 退出配置

内部网络的管理：可以限定对外网的访问，可以设定以 IP 地址或 MAC 地址为标识的用户对网络的具体权限。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

可以屏蔽一些网站为不可访问，封锁部分 IP 地址（例如部分行业对国外 IP 地址需要完全封锁）

对外的安全防范

对于网络监控与入侵防范，新 E 通基于 Netfilter 架构的防火墙有很好的防范措施。但是无论多么安全的防火墙，首先是管理上要保证系统的安全。新 E 通系统有两点需要特别指出：

a. 自己开发的专门的服务端口

这是一个是单独的通道，无论是内网主机、外网主机还是 DMZ 内主机都无法窃听到该通信，安全性显然很高，而且其协议是我们自己定义的，没有已知的黑客工具可以破解。

b. 通信过程加密

VPN 过程经过 168 位加密算法传输，这是国际上公认的加密算法。同时，也支持国家密码委员会指定的加密卡，这些加密算法是没有对外公开的。

B．对来自外部（和内部）攻击的反应能力

目前常见的来自外部的攻击方式主要有：

a. DOS（DDOS）攻击

（分布式）拒绝服务攻击是目前一种很普遍的攻击方式，在预防上也是非常困难的。目前防火墙对于这种攻击似乎没有太多的解决办法，主要是提高防火墙本身的健壮性（如增加缓冲区大小）。在新 E 通防火墙中（事实上几乎所有基于 Linux 建立的防火墙都有）中有一个防止 Syn flooding 攻击的选项：CONFIG_SYN_COOKIES，它是通过为每一个 Syn 建立一个缓冲（cookie）来分辨可信请求和不可信请求。另外对于 ICMP 攻击，例如 Ping 洪水，可以通过关闭 ICMP 回应来实现。 这个是非常基本的功能。

b. IP 假冒（IP spoofing）

IP 假冒是指一个非法的主机假冒内部的主机地址，骗取服务器的“信任”，从而达到对网络的攻击目的。

第一，防火墙设计上应该知道网络内外的 IP 地址分配，从而丢弃所有来自网络外部但却有内部地址的数据包。实际实现起来非常简单，只要在防火墙中打开 rp_filter 功能即可。

第二，防火墙将内网的实际地址隐蔽起来，外网很难知道内部的 IP 地址，攻击难度加大。

IP 假冒主要来自外部，对内网无需考虑此问题（其实同时内网的 IP 假冒情况也可以得到遏制）。

c. 特洛伊木马

防火墙本身预防木马比较简单，只要不让系统不能执行下载的程序即可。

一个需要说明的地方是必须指出的是，防火墙能抗特洛伊木马的攻击并不意味着内网主机也能防止木马攻击。事实上，内网主机可能会透过防火墙下载执行携带木马的程序而感染（如果该程序是通过压缩文件、邮件附件的方式，很可能跨过防火墙）。内网主机的在预防木马方面的安全性仍然需要主机自己解决（防火墙只能在内网主机感染木马以后起一定的防范作用）。 例如可以安装杀毒软件，现在许多软件都支持这种功能。

d. 口令字攻击

口令字攻击既可能来自外部，也可能来自内部，主要是来自内部。（在管理主机与防火墙通过单独接口通信的情况下，口令字攻击是不存在的）。

来自外部的攻击即用穷举的办法猜测防火墙管理的口令字，这个很容易解决，只要不把管理部分提供给外部接口即可。

内部的口令字攻击主要是穷举和嗅探，其中以嗅探危害最大。嗅探指监测网络截获管理主机给防火墙的口令字，如果口令字已加密，则解密得到口令字。一般采用一次性口令和禁止直接登录防火墙的措施来防止对口令字的攻击。新 E 通防火墙中有一个选项是禁止公网的地址访问本机。

e. 邮件诈骗

邮件诈骗是目前越来越突出的攻击方式。防火墙本身防止邮件诈骗非常简单，不接收任何邮件就可以了。然而

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029

象木马攻击一样，内网主机仍可收发邮件，邮件诈骗的危险仍然存在，其解决办法一个是内网主机本身采取措施防止邮件诈骗，另一个是在防火墙上做过滤。

常见问题解答

客户机不能被代理上网

1. 检查是否连接 Internet。直接在新 E 通上 ping 公网 IP 即可。例如 202.96.134.133。
2. 如新 E 通能上网而客户机不能，请检查 Licenses 是否设置正确。
3. 如果以上都正确，请检测网络物理连接；
4. 如果以上无误，请重新启动新 E 通。

如何知道有那些机器相连

1. 运行 route，可以看到其他机器的列表（以 IP 地址表示）。

MODEM 不自动拨号

1. 检测电话线是否正常。
2. MODEM 与电脑联接的串口线松动。
3. Modem 是否掉电。

MODEM 能拨号，但总不通

1. 查看是否有他人在使用与新 E 通相同的上网帐号。
2. 查看这个帐号是否过期。

ADSL 无法拨号上网

1. 首先检测您的网线是否使用正确。大多数 ADSL modem 使用普通网线直接与新 E 通 的 WAN1 相连。
2. 检测您的用户名和帐户是否正确或备盗用。一定要按照 ISP 给您的用户名和帐户输入。
3. 部分地区的 ADSL 用户，在终端设备突然掉电之后，不能马上拨号。需要等待一会才能重新连接。
4. 您可以在[APN GW/]模式下输入 **adsl-start** 重新连接。同样有效的命令还有 **adsl-stop**, **adsl-status**（查看状态）

不能启动

1. 查看电源是否工作。如果正常，前面板的电源指示灯应该亮绿。
2. 查看新 E 通前面板的系统自检灯是否正常。如果没有指示，说明是系统硬件故障，您需要与供应商或维修中心联系更换。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

新 E 通连接 Internet 前可以进入监管界面，但后来局域网工作站不能上网，也不能进入监管界面

1．检测同组内的子网与其它同组网内的网络地址相同，发生冲突。同一个 vdomian 内不同 vhost 的的机器不能在同样一个网段。

如何查看我现在新 E 通的公网 IP 地址

您可以使用 ifconfig 查看：

ifconfig

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0

eth0      Link encap:Ethernet  HWaddr 00:E0:4C:67:0D:22
          inet addr:176.16.10.1  Bcast:176.16.10.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:552386 errors:0 dropped:0 overruns:0 frame:0
          TX packets:759140 errors:0 dropped:0 overruns:0 carrier:0
          collisions:1228
          Interrupt:15 Base address:0xe000

eth1      Link encap:Ethernet  HWaddr 00:E0:4C:67:0D:21
          inet addr:172.31.250.250  Bcast:172.31.250.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:765931 errors:0 dropped:0 overruns:0 frame:0
          TX packets:547925 errors:0 dropped:0 overruns:0 carrier:0
```


地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888　传真：86-755-83268498
网址：www.sddata.com　邮编：518029

collisions:2708

ppp0 Link encap:Point-to-Point Protocol

inet addr:***218.17.67.147*** P-t-P:218.17.65.1 Mask:255.255.255.255

UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1492 Metric:1

RX packets:766024 errors:0 dropped:0 overruns:0 frame:0

TX packets:548002 errors:0 dropped:0 overruns:0 carrier:0

collisions:0

本例显示的 218.17.67.147 是此时新 E 通公网的 IP 地址。

如果您是 ADSL 连接 Internet，您可以使用 adsl-status 查看当前的 IP 地址。

[APN GW/]**adsl-status**

adsl-status: Link is up and running on interface ppp0

ppp0 Link encap:Point-to-Point Protocol

inet addr:218.17.67.147 P-t-P:218.17.65.1 Mask:255.255.255.255

UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1492 Metric:1

RX packets:766486 errors:0 dropped:0 overruns:0 frame:0

TX packets:548359 errors:0 dropped:0 overruns:0 carrier:0

collisions:0

如何打开 Telnet 让远程技术人员登录

您可以使用

[APN GW/]**advconf telnet start**

打开 Telnet 功能。此时您可以查看当前新 E 通的公网地址，这样就可以让远程的技术人员登录新 E 通进行调试。

注意您如果需要一直打开 telnet 功能，需要记住更改您的密码。

地址：中国深圳市福田区笋岗路中成大厦十九楼
电话：86-755-83268888 传真：86-755-83268498
网址：www.sddata.com 邮编：518029